Technical Report **1754**
September 1997

Asynchronous Transfer Mode (ATM)

R. L. Ehlen

Naval Command, Control and Ocean Surveillance Center
RDT&E Division, San Diego, CA 92152-5001

Table of Contents

1 Introduction

As high speed data communication, video on demand or multimedia applications become more and more common, networks have to be flexible enough to support all new services and to guarantee a specified Quality of Service (QoS) and network performance. Networks (e.g., Ethernet, FDDI, DQDB, or X.25) built in the past were developed for specialized applications (e.g., data), and none of them have all of the following features necessary to support future broadband communication services:

- Flexible bandwidth allocation;
- Capability to integrate all services;
- Fast and efficient transmission of constant and variable bit rate traffic;
- Low information loss and delay times;
- Fast and efficient network control;
- Flexible and dynamic network configuration;
- Flexible, efficient and fast network management;
- Evolutionary development with integration of most existing services.

Asynchronous Transfer Mode (ATM) is a new technology that can fulfill the requirements of diverse user applications such as voice, video, and data and interoperate with most of the current network technologies and protocols; however, the specification of ATM networks has not been completed.

ATM has been choosen by telecommunication companies as the transfer mode for future broadband networks. Research, development, and testing of ATM networks are taking place worldwide. So ATM is a very fastly evolving commercial-off-the-shelf (COTS) technology used in LANs, MANs, and WANs. The ability to integrate data, voice and video into a single network also makes ATM an interesting technology to be used in a military environment.

The goal of this report is to describe the fast evolving ATM technology, with special emphasis on new standards, research results and developments. I wrote this report when I was a German Exchange Engineer at Code D827 of the Naval Reserach and Development Center at San Diego, CA. My intention was not to describe everything in detail or all basic features of ATM; otherwise I would still be writing this report because too much exists. I assume that the reader has knowledge about networking and basic functions of ATM. This report should be used like a dictionary to get an overview of the ATM technology. For further details, it is necessary to look into the papers listed in the reference list.

Chapters 1 to 8 describe the basic features of ATM networks. The topics discussed are relatively finalized and little has changed to date. Chapters 9 to 13 describe the new ATM technology areas, including some information that is only a few months old. ATM and its companion technologies are being developed by the International Telecommunications Union, the ATM Forum, and the Internet Engineering Task Force. Many of these technologies are described by these organizations through the use of Specifications and Requests for Comments (RFCs). Chapter 16 provides a list of the RFCs and Specifications crucial to the development of ATM. Chapter 18 provides a list of ATM-specific acronyms. Although not all the acronyms listed were explicitly described in this report, they are necessary for reading other ATM literatures. Chapter 19 provides a list of references crucial to understanding the ATM technology. In many cases, Internet addresses and links are included.

As English is not my native language I would like to thank Allen Shum (code 827) for reading the draft of this paper and correcting my grammatical mistakes.

In Germany I work as an electrical engineer for the German government at the Federal Office for Defense Technology and Procurement (Bundesamt für Wehrtechnik und Beschaffung, BWB). More information (e.g., organization) about my office is available on the English homepage at http://www.bundeswehr.de/bwb/english/index-e.htm.

Address in Germany:

Bundesamt für Wehrtechnik und Beschaffung

Postfach 7360

56057 Koblenz

Germany

2 B - ISDN

Many networks designed for data transmission or telephony exist. They have been evolving from analog to digital (e.g., ISDN) and from small bandwidth to broadband systems (e.g., B-ISDN). The standardization organization ITU-T classifies the current communication networks as follows:

- ❒ Circuit-switched networks;
- ❒ Message-switched networks;
- ❒ Packet-switched networks:
  - Datagram packet switching,
  - Virtual-circuit packet switching.

It should be noted that the distinction between message- and packet-switched networks is rather fuzzy. Message switching generally refers to the transfer of an entire unit of information or message meaningful to a user, with no upper limit on the size of a message; packet switching refers to the transfer of unit of information that has a upper limit on its size. Still, many people do not acknowledge such artificial delineation and regard message switching as a specialized form of packet switching.

In ISDN, the functions and features of circuit- and packet-switched networks are included to support voice, low-speed data, and low-quality video conferencing services. The base is a 64-kbit/s channel. A user may request some integer multiple (up to 24) of the base 64 kbits/sec channel. Four physical interfaces, two basic rate and two primary rate interfaces, are specified for a speed up to 1.536 Mbit/s (T1 in the U.S.) or up to 2.048 Mbit/s (E1 in Europe). The interfaces consist of a combination of bearer (B) channel with a 64-kbit/s transmission rate, high-speed bearer (H) channel with a higher bandwidth (e.g., H0: 384 kbit/s), and a dialogue channel (D channel) with 16 kbit/s. The B-ISDN offers a higher rate to support all services (ITU-T Recommendation I.121) for constant or variable, connection-oriented or connectionless transfer of data, voice and video. The ITU-T classifies all possible broadband applications into 4 categories to support not only the current, but also future applications:

1. Conversational services;
2. Retrieval services;
3. Messaging services;
4. Distributional services:
   - without user-individual presentation control;
   - with user-individual presentation control.

B-ISDN will support many different types of services and applications. These services can be characterized by the following attributes:

- High bandwidth;
- Bandwidth on demand;
- Varying Quality-of-Service (QoS) parameters;
- Guaranteed service levels;
- Point-to-point, point-to-multipoint, multipoint-to-multipoint connections;
- Constant- or variable-bit-rate services;

- Connection-oriented or connectionless services.

B-ISDN refers to a network that can support all these future diverse broadband services, but how is B-ISDN being implemented? What is ATM?

3 ATM

3.1 General Discussion

ATM is the only technology that can support broadband diverse services and applications such as video, voice, and data. It is a packet-switched technology that segments user information, whether it contains voice, video, or data, into small fixed-size packets called cells, and these cells are transported through a single set of transmission resources.

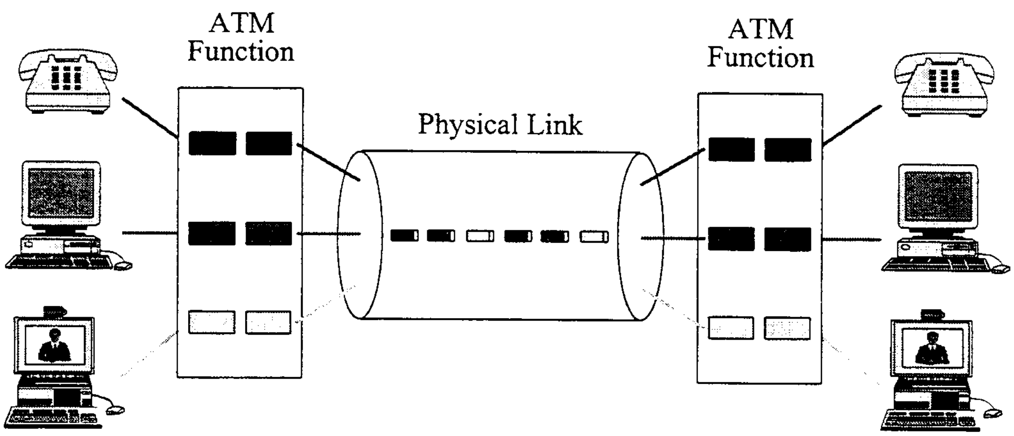


Figure 3.1: Service integration using ATM

Each cell has 53 bytes, with a 5-byte header/descriptor for protocol execution and 48 bytes for payload.

Header (5 bytes)	Payload (48 bytes)

Figure 3.2: ATM packets

ATM is a protocol structure, which roughly corresponds to the lower four layers of the OSI Reference Model, but the structure of the ATM protocol is different from the OSI structure.

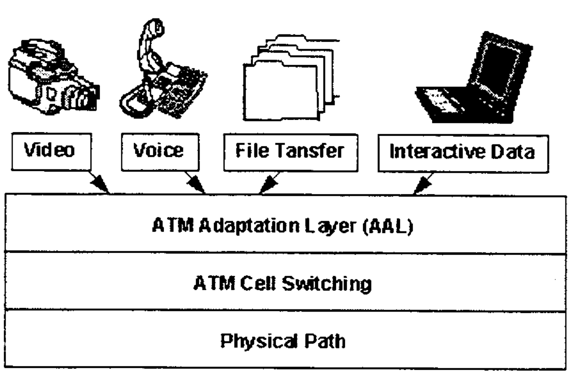


Figure 3.3: ATM services

The 3 layers in an ATM structure are

- ATM Adaptation Layer (AAL);
- ATM Layer;
- Physical Layer.

ATM has no special structure corresponding to the layer 5 to 7 of the OSI model. Most of the known protocol stacks and applications can be used to transfer all types of information.

This ATM architecture fits perfectly into the B-ISDN Protocol Reference Model for the user part and the control part.

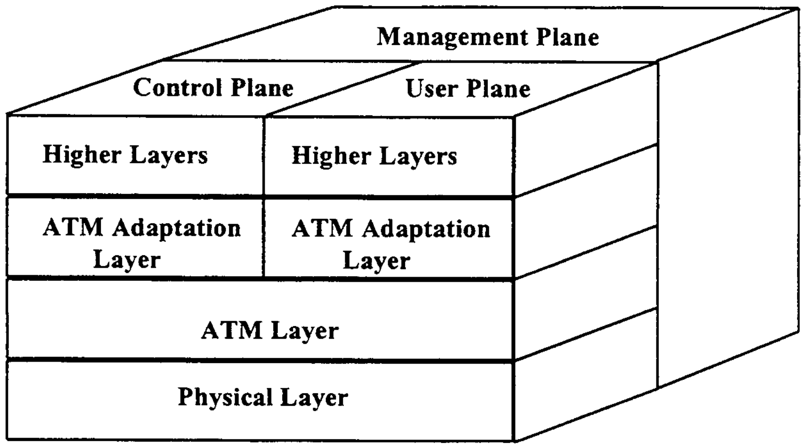


Figure 3.4: B-ISDN Protocol Reference Model

How the 5-byte ATM cell header looks like depends on the use of the cells and whether the cells are transported between an ATM end user and an ATM switch (User-Network) or between two ATM switches (Network-Network) (Fig. 3.5).

The corresponding available interfaces and the cell formats are:

- UNI (user-to-network interface) or
- NNI (network-to-network interface).

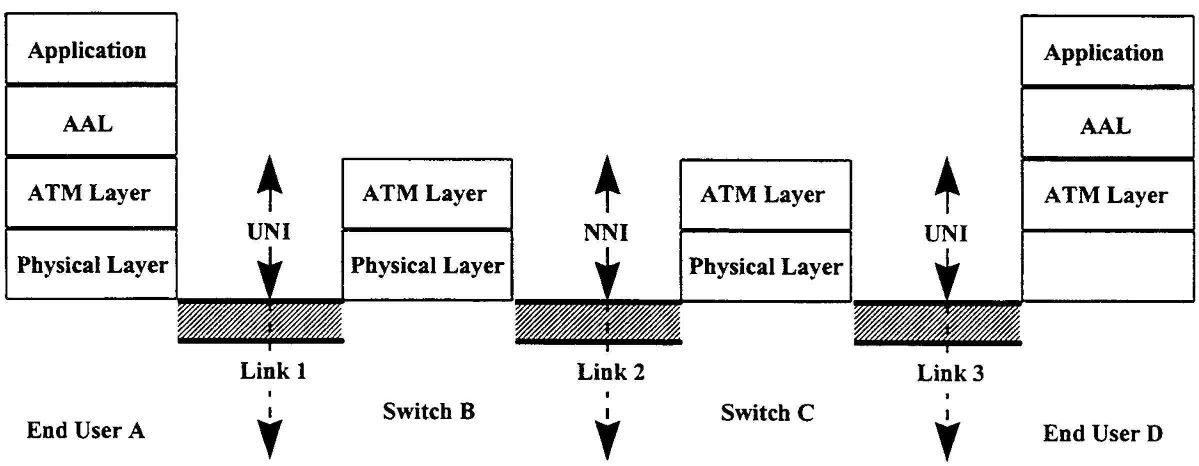


Figure 3.5: ATM network

The following fields are part of an ATM-cell:

- Virtual path identifier (VPI);
- Virtual channel identifier (VCI);
- Payload type (PT);
- Cell loss priority (CLP);
- Header error check (HEC);
- Generic flow control (GFC).

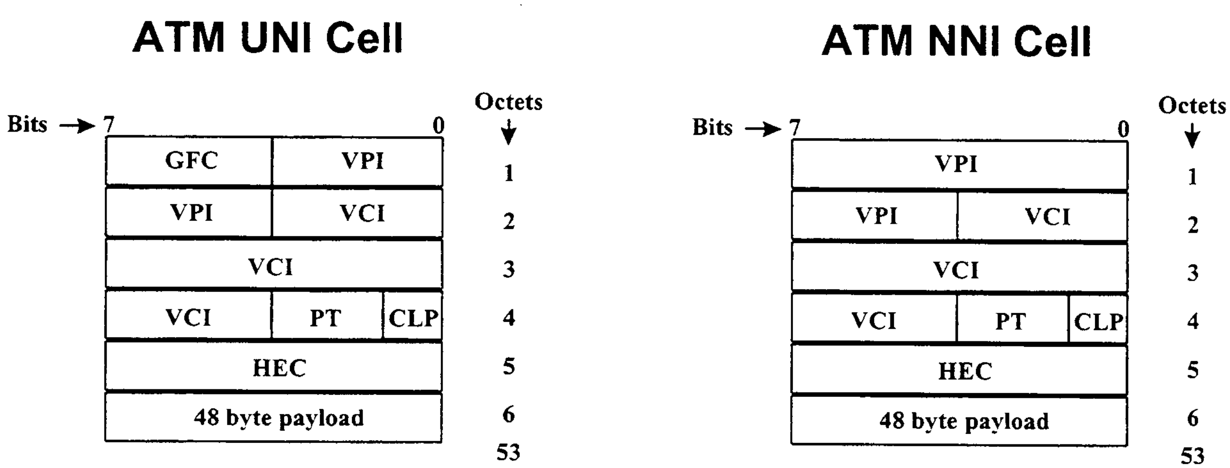


Figure 3.6: ATM UNI Cell and NNI Cell

The only difference between an ATM UNI cell and an ATM NNI cell is that the UNI cell header contains a 4-bit GFC field, which provides a framework for flow control between an ATM end station and the network. The 8-bit HEC field is used for discarding cells with corrupted headers and cell delineation. It provides single-bit error correction and a low probability of delivering corrupted cells.

Every layer in the ATM structure provides certain set of functionalities to support all services. An ATM adaptation layer (AAL) is divided into two sublayers:

- Convergence Sublayer (CS) and
- Segmentation and Reassembly (SAR).

The convergence sublayer is service-dependent, and provides error control and sequencing of information. SAR is service-independent, and divides a CS message or protocol data unit into 48-byte segments as cell payloads for the ATM layer. The ATM layer provides the switching and multiplexing of traffic. An ATM network must support end-to-end ATM layer connectivity between end stations at very high speed, and consequentially, must be very streamlined and cannot provide many of the functionalities and services needed by user applications. The role of the ATM adaptation layer is to provide the necessary services needed by an application that are not provided by an ATM network, namely, by the physical and ATM layers. Since different applications require very different services, several AALs are defined. The role of the physical layer is to transport cells between two ATM layers.

The routing information of each cell is included two fields of the header: virtual path identifier (VPI) and virtual channel identifier (VCI). With this information, the cells can be routed through the network from one switch to another. Each switch overwrites, for every arriving cell, new VPI and VCI. Cells are routed over two hierarchies of connections, virtual path and virtual channel connections, which are defined by ITU-T Recommendation I.113. The objective of having two hierarchies of connections is to facilitate switching and offer flexibility. The salient features of the two hierarchies are as follows:

- VC: A concept to describe a virtual communication channel for the unidirectional transport of ATM cells.

- VP: A concept to describe a virtual communication path consisting of multiple virtual channels for the unidirectional transport of ATM cells.

The following table summarizes the functions of the layers defined in the B-ISDN Protocol Reference Model:

Higher Layers

Layer		Functions
Higher layers		Higher layer functions
AAL	Convergence sublayer	Service specific (SSCS) Common part (CPCS)
	SAR sublayer	Segmentation and reassembly
ATM		Generic flow control Cell header generation/extraction Cell VPI/VCI translation Cell multiplexing/demultiplexing
Physical	Transmission convergence (TC) sublayer	Cell rate decoupling HEC sequence generation/verification Cell delineation Transmission frame adaptation Transmission frame generation/recovery
	Physical medium dependent (PMD) sublayer	Bit timing Physical medium

Figure 3.7: Functions of the ATM adaptation layer, ATM layer, and physical layer

This chapter describes the layers in detail.

3.2 ATM Layer

The role of the ATM layer is to transport cells between peer ATM entities. An ATM layer generates a 5-byte header to each payload received from its user (e.g., AAL) at the originating end station and sends it to a physical layer below for transport.

More specifically, the ATM layer performs the following functions:

- Cell structure and encoding;
- Services expected from the physical layer;
- Services provided to ATM layer users;
- ATM layer management;
- Traffic and congestion control.

Cell structure and encoding refers to the generation of the cell header, which is used for protocol execution by ATM layer peers. A cell header can identify the connection to which a cell belongs through the VPI and VCI; can specify flow control from end stations to the network by limiting their effective ATM layer transport capacity with the GFC field. The payload type, whether the cell carries user or operation, administration and maintenance (OAM) data, can be identified with the PTI field. The CLP field can be used by the network or an ATM end user for selective discarding of cells and flow control.

The ATM layer management performs OAM functions. Although five OAM functions (performance monitoring; defect and failure detection; system protection; failure or performance information; fault localization) have been defined, typically only performance and fault management are provided by the ATM layer.

3.3 ATM Adaptation Layer (AAL)

An ATM network provides an end-to-end connection between end stations through the ATM layer. The ATM layer can provide only minimal functionalities. This simplicity in the transmission is necessary for high-speed transfers, and, as a result, the following functions are not included in the ATM layer:

- Timing Information such as the frequency of the service clock;
- Error control;
- Cell delay variation control.

The AAL is used between the ATM layer and the next higher layer; it transforms traffic stream from the higher layer into a stream of 48-byte cell payloads and provides some of the services needed by the higher layer. Since it is not advisable to support all applications and user requirements in one single AAL, several AALs are defined, with each AAL providing a unique set of functions needed by a particular service class.

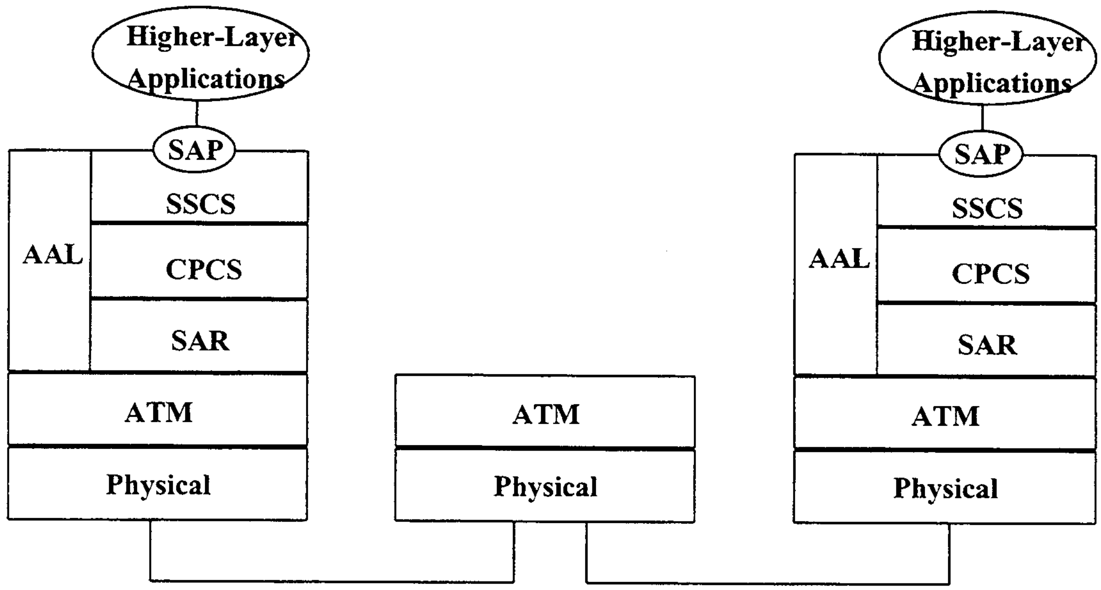


Figure 3.8: AAL structure

The ITU-T classifies B-ISDN services according to the following parameters:

- Timing relationship between source and destination (required or not required);
- Bit rate characteristic (constant or variable);
- Connection mode (connection-oriented (CO) or connectionless (CL) services).

Every service in the B-ISDN is categorized into a service class. Based on the above parameters, six service classes are defined:

- ❒ Class A: CBR, CO, timing — e.g., 64 kb voice, CBR video;
- ❒ Class B: VBR, CO, timing — e.g., VBR encoded video;
- ❒ Class C: VBR, CO, no timing — e.g., CO data transfer;
- ❒ Class D: VBR, CL, no timing — e.g., CL data transfer;
- ❒ Class X: AAL, traffic type (CBR or VBR) and timing is defined by the user;
- ❒ Class Y: VBR, CO, no timing; possibility for a user to change the transfer characteristics after connection establishment.

The ATM Forum and the ITU-T have defined the following ATM adaptation layers to provide services for the different service classes:

- ❒ AAL 0: a user-defined AAL to provide services for Class X traffic;

❒ AAL 1: CRC-3 check, parity check, cs (continue or start) with timing relationship, CBR, CO;

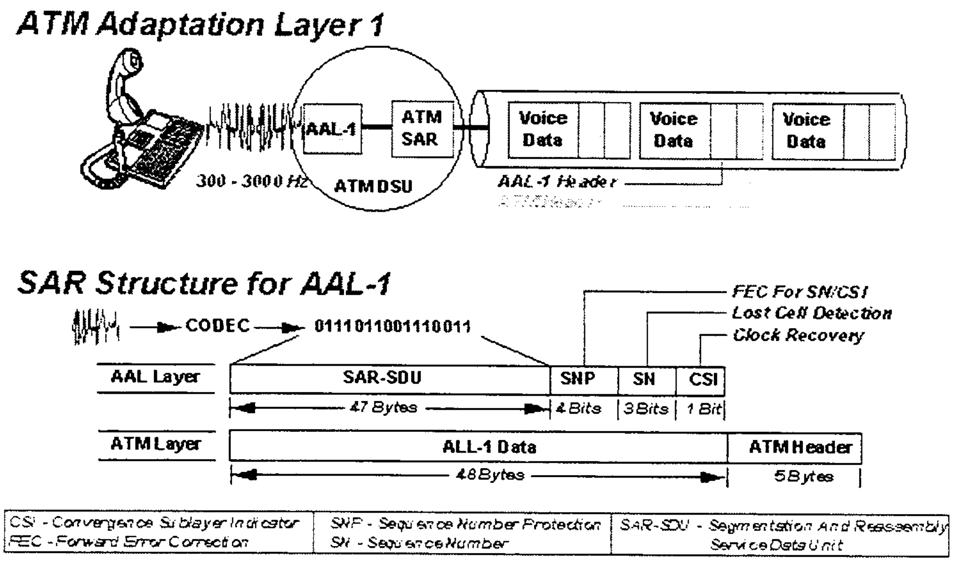


Figure 3.9: AAL 1

❒ AAL 2: Standardization not completed by ITU-T, developed to recover timing relationship between end-to-end-applications, VBR, CO;

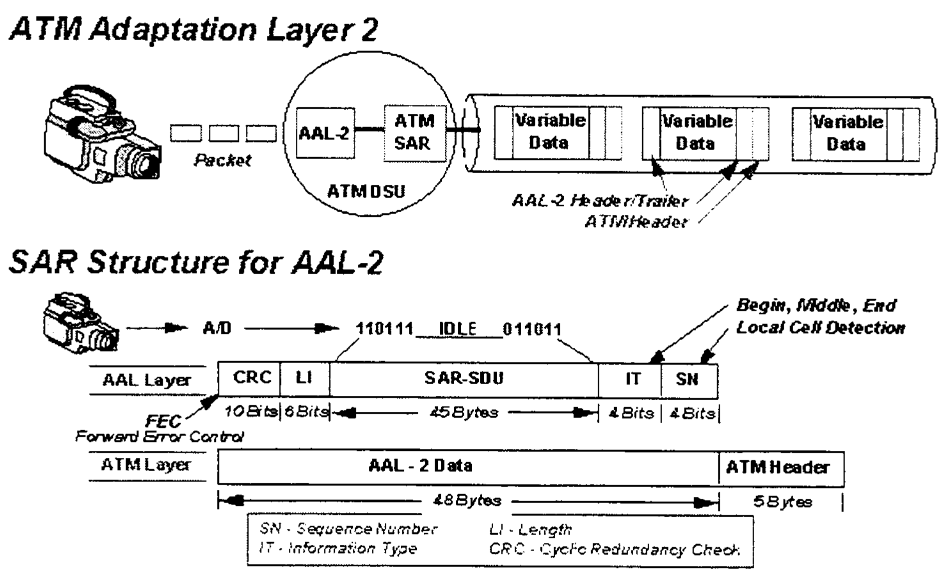


Figure 3.10: AAL 2

❑ AAL 3/4: CRC-10 check, no end-to-end timing, VBR, CO or CL;

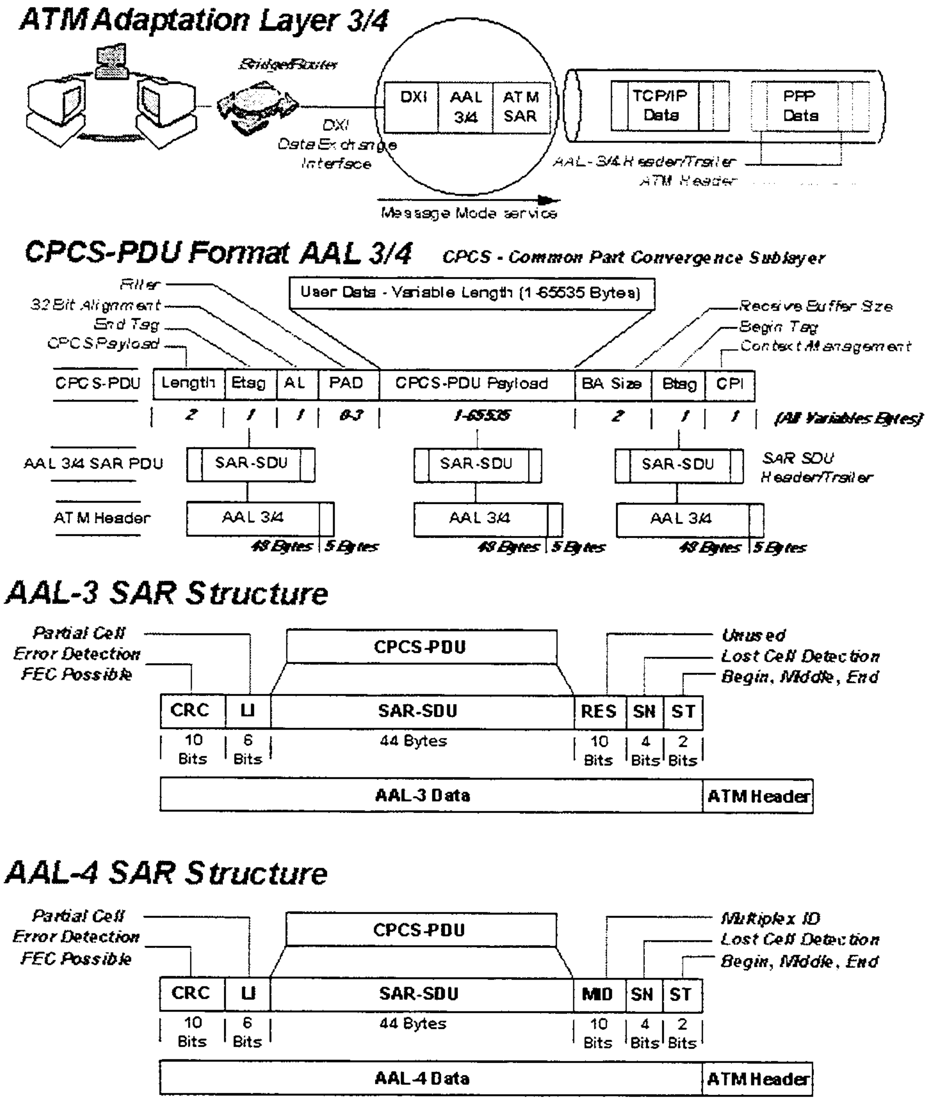


Figure 3.11: AAL 3/4

- AAL 5: CRC-32 check, no timing, VBR, CO oder CL;

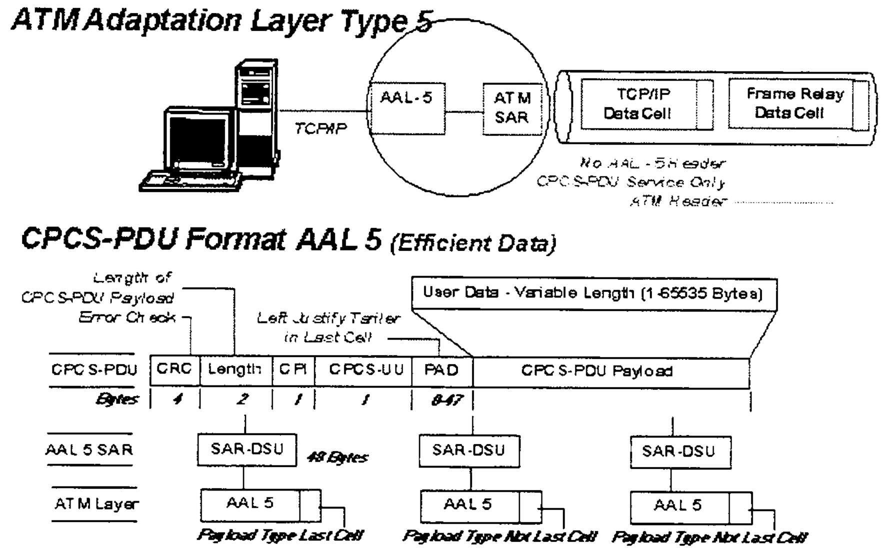


Figure 3.12: AAL 5

- AAL6: Proposal by the ITU-T to define VBR service for low-bit rate voice traffic between wireless base stations and mobile switch centers; the proposal also defines voice compression and silence suppression.

It looks as if AAL3/4 and AAL 5 are the same: both are defined for VBR connection-oriented, as well as connectionless, traffic. There are, in fact, important differences. AAL3/4 was defined first, and can multiplex the traffic from different applications serviced by the AAL onto a single ATM connection; however, this nice feature increases the overhead by another 4 bytes, so that the effective payload is only 44 bytes. AAL5 eliminates this additional overhead so that the maximum available for application protocol data units is 48 bytes. Also, AAL5 provides a much more robust error detection as a result of using a powerful 32-bit CRC. The following table summarizes the relationship between the service classes and the AALs:

	Class A	Class B	Class C	Class D	Class X
Timing between source and destination	Required	Required	Not required	Not required	User defined
Bit rate	CBR	VBR	VBR	VBR	VBR
Connection mode	CO	CO	CO	CLN	CO
AAL type	AAL1	AAL2	AAL3/4 and 5	AAL3/4 and 5	AAL0

Figure 3.13: AALs and their corresponding service classes

Figure 3.14 shows how to use ATM to support integrated services:

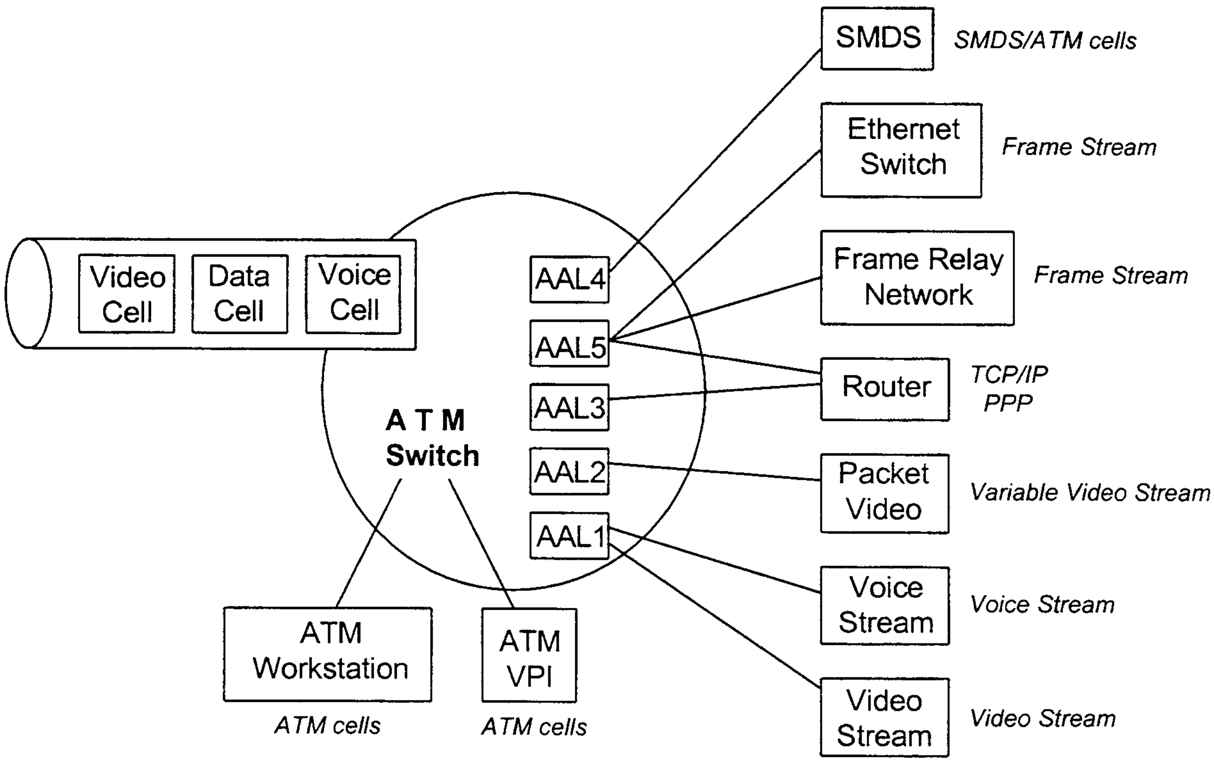


Figure 3.14: ATM integrated services

3.4 ATM Physical Layer

The physical layer is divided into two sublayers:

- ❒ Transmission convergence sublayer and
- ❒ Physical media dependent sublayer.

ATM layer	
Transmission convergence sublayer	
	HEC generation and checking
	Cell delineation
	Transmission frame adaption
	Decoupling of cell rate
Physical media dependent sublayer	
	Encoding for transmission
	Timing and synchronization
	Transmission (electrical/optical)

Figure 3.15: Structure of the physical layer

The role of the physical layer is to perform functions necessary to transport cells over a physical medium. Many ATM-specific physical layer interfaces exist. The most important ones are:

- SONET/SDH - ATM Interface: specified for Sonet: (810-byte frame, 125 microsec, basis structure is STS-1 with 51.84 Mbit/s);
- PDH Interfaces: plesiochronous (nearly synchronous);
    - Direct mapping,
    - Mapping over the PLCP (physical layer convergence protocol) in a 125 microsec-system with DS1 frame and 193 bit length,
- 155 Mbit/s fiber channel PMD physical interface with a 27-cell frame;
- Cell stream ATM physical layer interface: 25.6 Mbit/s interface on basis UTP-3 and as 100 Mbit/s Taxi for FDDI.

4 Source Characterization

4.1 General Discussion

An application can be characterized in terms of the traffic that it generates and its Quality-of-Service (QoS) requirements. The following definition of QoS is given by the ITU-T in Recommendation I.350:

> ☞ QoS is the collective effect of service performances which determine the degree of satisfaction of a user of the specific service.

4.2 QoS Parameters

ATM is a connection-oriented packet-switching network, and its performance can be measured in terms of two categories of QoS:

- Call control QoS, which refers to the signaling performance rendered by the network, and
- Information transfer QoS, which refers to the degree that the network can provide the quality of services required by user applications.

The three most important call control quality of service parameters are:

- Connection setup delay;
- Connection release delay;
- Connection acceptance propability (blocking probability).

Connection setup delay refers to the time interval between a call setup message is generated and the corresponding call setup acknowledge message is received, excluding the response time of the called user. The longest permissible connection spans 27,500 km. Recommendation I.352 of the ITU-T specifies that the average delay should be less than 4.5 msec and 95 % of the delay should be less than 8.35 msec. Connection release delay refers to the time interval between the generation of a call release message and the receipt of the corresponding call release acknowledge message. This delay should be less than 300 msec and 95 % of the delay should be less than 850 msec. Connection acceptance probability is the ratio between the number of call attempts and the number of calls accepted by the network during a long time period.

The most important information transfer parameters are:

- BER: bit error ratio;
- CLR: cell loss ratio;
- CIR: cell insertion ratio;
- CTD: end-to-end cell transfer delay;
- CDV: cell delay variation (jitter);
- skew.

CTD has several components:

- Coding delay;

- Packetization delay;
- Propagation delay;
- Transmission delay;
- Switching delay;
- Queuing delay;
- Reassembly delay.

An application may be categorized into one of the following service classes defined by the ATM Forum:

- CBR (constant bit rate) ⇔ class A
- RT-VBR (real-time variable bit rate) ⇔ class B
- NRT-VBR (non-real-time variable bit rate) ⇔ class C, D
- ABR (available bit rate) ⇔ class Y
- UBR (unspecified bit rate) ⇔ class D

These traffic classes are used in various ATM Forum specifications, e.g., Traffic Management Specification (Version 4.0). Other organizations describe essentially the same topics, e.g., ITU-T Recommendation I.371 --Traffic Control and Congestion Control in B-ISDN.

ATM-Forum TM 4.0 "ATM Service Category"	ITU-T I.371 ATM Transfer Capability	Typical use
Constant Bit Rate (CBR)	Deterministic Bit Rate (DBR)	Real-time, QoS guarantees
Real-Time Variable Bit Rate (RT-VBR)	(for further study)	Statistical mux, real-time
Non-Real-Time Variable Bit Rate (NRT-VBR)	Statistical Bit Rate (SBR)	Statistical mux
Available Bit Rate (ABR)	Available Bit Rate (ABR)	Resource exploitation, feed-back control
Unspecified Bit Rate (UBR)	(no equivalent)	Best efford, no guarantees
(no equivalent)	ATM BlockTransfer (ABT)	Burst level feedback control

Figure 4.1: Standards and their definitions

Differentiation of traffic classes is necessary to efficiently support diverse applications with very different bit rate characteristics and performance requirements. The means for an application to identify its traffic class is through call admission control. During call admission control, an end user describes to the network its traffic charateristics and service requirements in terms of a number of traffic and QoS parameters. The network then determines whether there are sufficient resources to maintain the QoS of the requesting end user as well as the already established connections. If so, the call request is granted and the network will probabilistically provide service guarantees to the end user as long as the end user generates traffic consistent with the traffic parameters specified during call set up; that is, a "traffic contract" is established between the end user and the network.

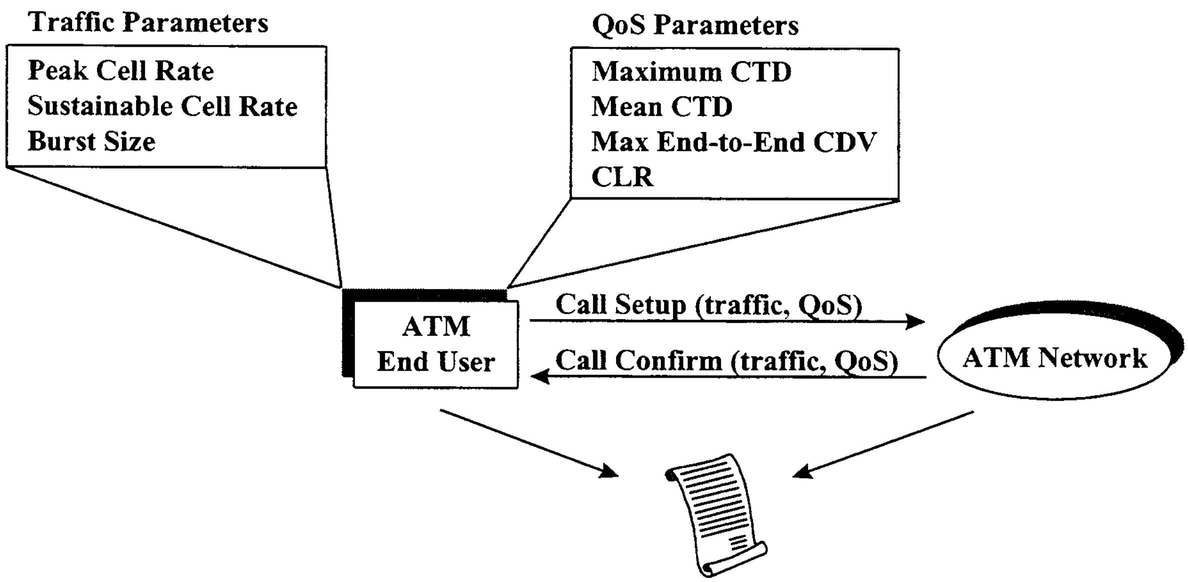


Figure 4.2: ATM traffic contract

The following table shows several typical applications and their ATM service categories.

Application Area	CBR	RT-VBR	NRT-VBR	ABR	UBR
Critical Data	**	*	***	*	n/s
LAN Interconnect LAN Emulation	*	*	**	***	**
Data transport/Interworking (IP-FR-SMDS)	*	*	**	***	**
Circuit emulation -PBX	***	**	n/s	n/s	n/s
POTS/ISDN-Video Conference	***			n/s	n/s
Compressed audio	*	***	**	**	*
Video distribution	***	**	*	n/s	n/s
Interactive multimedia	***	***	**	**	*

Explanation: optimum: *** good: ** fair: * not suitable: n/s

Figure 4.3: Applications and their ATM service categories

It is also necessary to specify the QoS parameters associated with these service classes.

Feature	Constant Bit Rate (CBR)	Real-time Variable Bit Rate (VBR)	Non-Real-Time VBR	Available Bit Rate (ABR)	Unspecified Bit Rate (UBR)
Cell Delay Variation (Jitter)	Specifiable	Specifiable	Not specifiable	Not specifiable	Not specifiable
Max Cell Transit Delay (Latency)	Specifiable	Specifiable	For further study	Not specifiable	Not specifiable
Cell Loss Ratio (% dropped)	Specifiable	Specifiable	Specifiable	Specifiable	Not specifiable
Cell Error Ratio (% erred)	Specifiable	Specifiable	Specifiable	Specifiable	Not specifiable

Figure 4.4: ATM service classes and QoS parameters

5 ATM-Interfaces

5.1 General Discussion

An interface specifies the permissible behaviors exhibited accross a demarcation or reference point between different entities. The ATM Forum has specified the following interfaces:

- ❒ DXI (Data Exchange Interface);
- ❒ B-ICI (Broadband Intercarrier Interface);
- ❒ UNI (User-to-Network Interface);
- ❒ NNI (Network-to-Network Interface);
- ❒ PNNI (Private NNI);
- ❒ ILMI (Integrated Local Management Interface).

The goal of these interfaces is to provide a standardized means through which different components of ATM networks, e.g., ATM end stations, ATM switches, service interfaces, can communicate and interoperate.

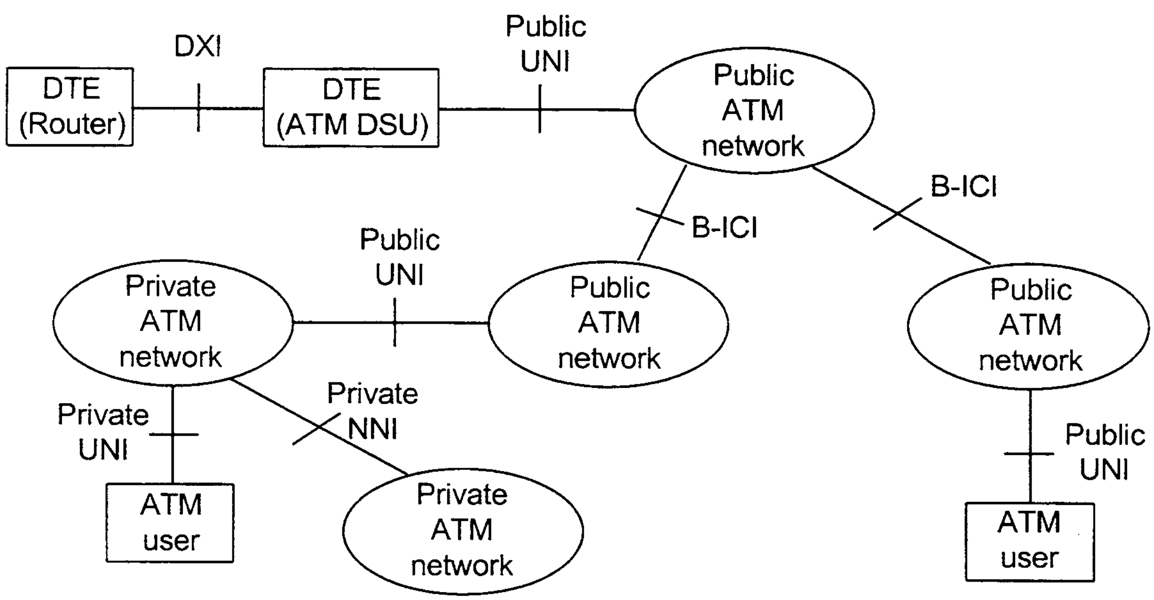


Figure 5.1: ATM Forum interfaces

UNI is an interface between a user and a network, either private or public. NNI is the interface between two networks. For public networks, it is called NNI to distinguish it from the interfaces, referred to as P-NNIs, between ATM switches in a private ATM network. DXI specifies how to connect a router to a data terminal equipment (DTE) and a data communication equipment (DCE) to an ATM-network, and vice versa. B-ICI is a carrier-to-carrier interface, and may include physical layer and higher layer services interfaces such as switched multi-megabit data service (SMDS) and frame relay. ILMI provides a means to establish switch-to-switch configuration and to exchange status and control information across a UNI.

5.2 UNI Specification

The UNI specification can be categorized into four sections:

- Physical layer interfaces;
- ATM layer;
- ILMI;
- UNI signaling.

The physical layer interfaces were discussed in a previous chapter, and UNI signaling can be found in the next chapter. This chapter will focus on the ATM layer.

An ATM connection can be preconfigured manually or established dynamically through signaling. Dynamically and manually established connections are referred to as switched virtual connnections (SVCs) and permanent virtual connections (PVCs), respectively. An ATM connection permits the transfer of cells between two ATM end users, which are uniquely identified by ATM addresses. There are two address formats:

- Public ATM networks: use E.164;
- Private ATM networks: use OSI-NSAP (network service access point).

The NSAP address format is based on the concept of hierarchical domains. RFC 1237 describes NSAP in more details.

The E.164 format contains a 20-byte ATM address, which is divided into two parts:

- Initial Domain Part (IDP) and
- Domain-Specific Part (DSP).

The IDP specifies a subdomain of the global address space, and consists of an authority and format identifer (AFI) and the initial domain identifier (IDI). The AFI specifies the format of the IDI and the abstract syntax of the DSP.

<table>
<tr><td colspan="2">IDP</td><td colspan="3">DSP</td></tr>
<tr><td>AFI</td><td>IDI</td><td>High order DSP</td><td>ESI</td><td>Selector</td></tr>
</table>

Figure 5.2: ATM address format

Three different AFIs are defined:

- Data country code (DCC);
- International code designator (ICD) and
- E164 ATM address (E.164).

The UNI 3.1 specification defines the traffic classes A,C and X and their corresponding AALs, namely, AAL-1, AAL-3/4 and AAL-5. The characteristics of a traffic class may be defined in terms of a number of traffic parameters:

- PCR (peak cell rate);
- MCR (minimum cell rate);

- ❒ SCR (susteinable cell rate);
- ❒ BT (burst tolerance).

UNI 3.1 defines the following QoS classes:

- ❒ QoS class 0: supports service with no exlicit specified requirement;
- ❒ QoS class 1: supports QoS requirements of the B-ISDN-class A;
- ❒ QoS class 2: supports QoS requirements of the B-ISDN-class B;
- ❒ QoS class 3: supports QoS requirements of the B-ISDN-class C;
- ❒ QoS class 4: supports QoS requirements of the B-ISDN-class D.

In the next version of UNI specification, the ATM Forum will specify the following service classes, which are necessary for traffic management:

- CBR (constant bit rate);
- RT-VBR (real-time variable bit rate);
- NRT-VBR (non-real-time variable bit rate);
- ABR (available bit rate);
- UBR (unspecified bit rate).

For a variable bandwidth allocation, the following QoS parameters of a connection must be specified:

- Peak-to-peak CDV;
- Maximum CTD;
- CLR;
- CER.

5.3 DXI Specification

The data exchange interface (DXI) was designed to provide installed equipment access to ATM networks without upgrades. DXI allows DTE (e.g., router) and DCE to cooperate with ATM networks. The DXI framework defines the protocols for a DTE to transport a DTE-SDU from one DTE to another DTE via an ATM network (Fig. 5.3). The DXI specification includes the definition of a data link control protocol, the local management interface (LMI), and the management information base (MIB). The physical layers which handle the data transfer between DTE and DCE are also defined in the DXI. The LMI defines the protocol to exchange (DXI-, AAL- and ATM-UNI-specific) management information across a DXI. LMI also defines the interface between a management station (which runs a SNMP) and a switch (which runs the ILMI protocol). The ATM DXI is managed by the DTE through the LMI.

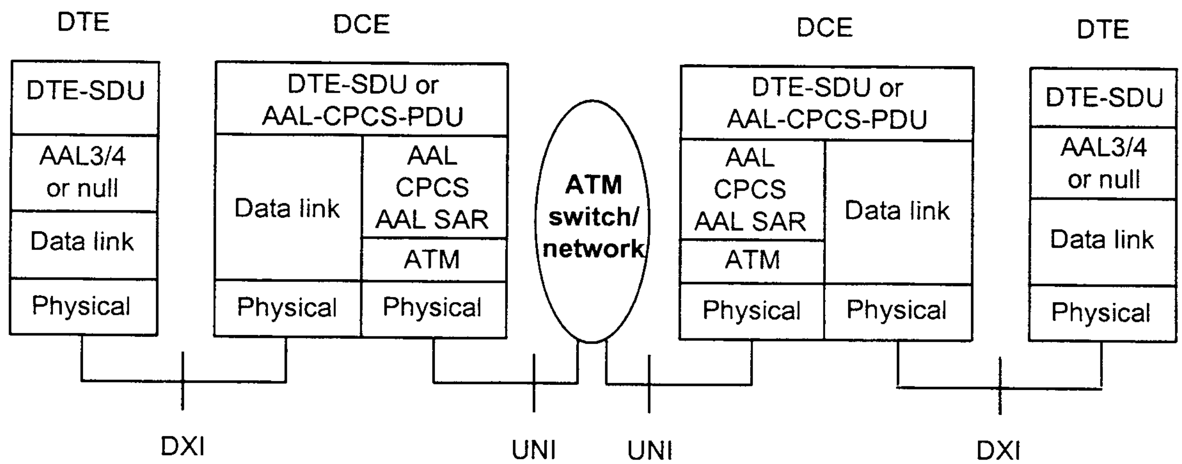


Figure 5.3: DXI framework

DXI supports V.35, RS 449, and HSSI for a wide range of bandwidth up to 50 Mbit/s and defines a data link control protocol.

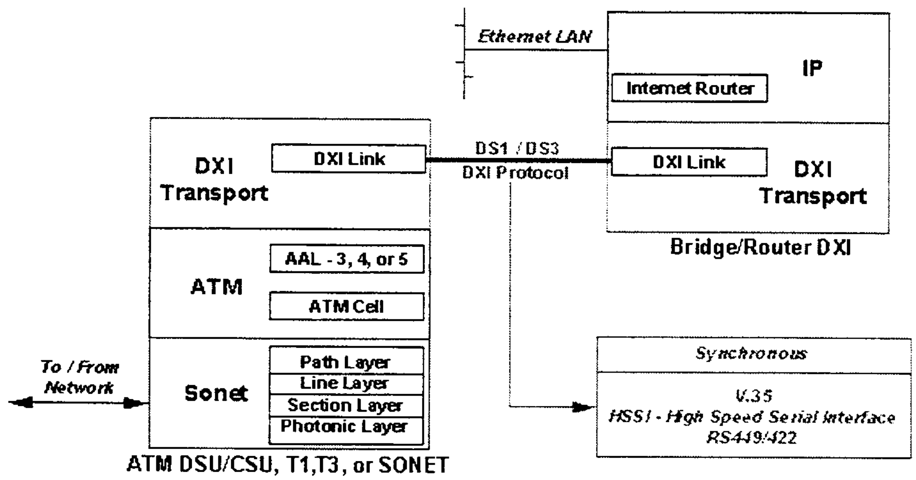


Figure 5.4: DXI protocol

The specific DXI protocol actions executed depend on the selected operational mode. There are three operational modes: 1a, 1b, or 2. The differences among these modes are the AALs used, the place where encapsulation occurs, the length of the DXI header, and the use of CRC. These differences are outlined below:

- Mode 1a transports DTE-SDUs using the AAL 5 common part convergence and SAR sublayers. The DCE encapsulates DTE-SDUs into AAL 5 CPCS-PDUs with CRC-16 and a 2-byte DXI header;
- Mode 1b transports DTE-SDUs using AAL3/4; DTE encapsulates a DTE-SDU into AAL3/4 CPCS-PDUs with CRC-16 and a 2-byte DXI header;
- Mode 2 operates like mode 1b, but the DTE encapsulates a DTE-SDU into AAL3/4 CPCS-SDUs with CRC-32 and a 4-byte DXI header.

The next figure shows the protocol architecture for the various operational modes and their supporting AALs:

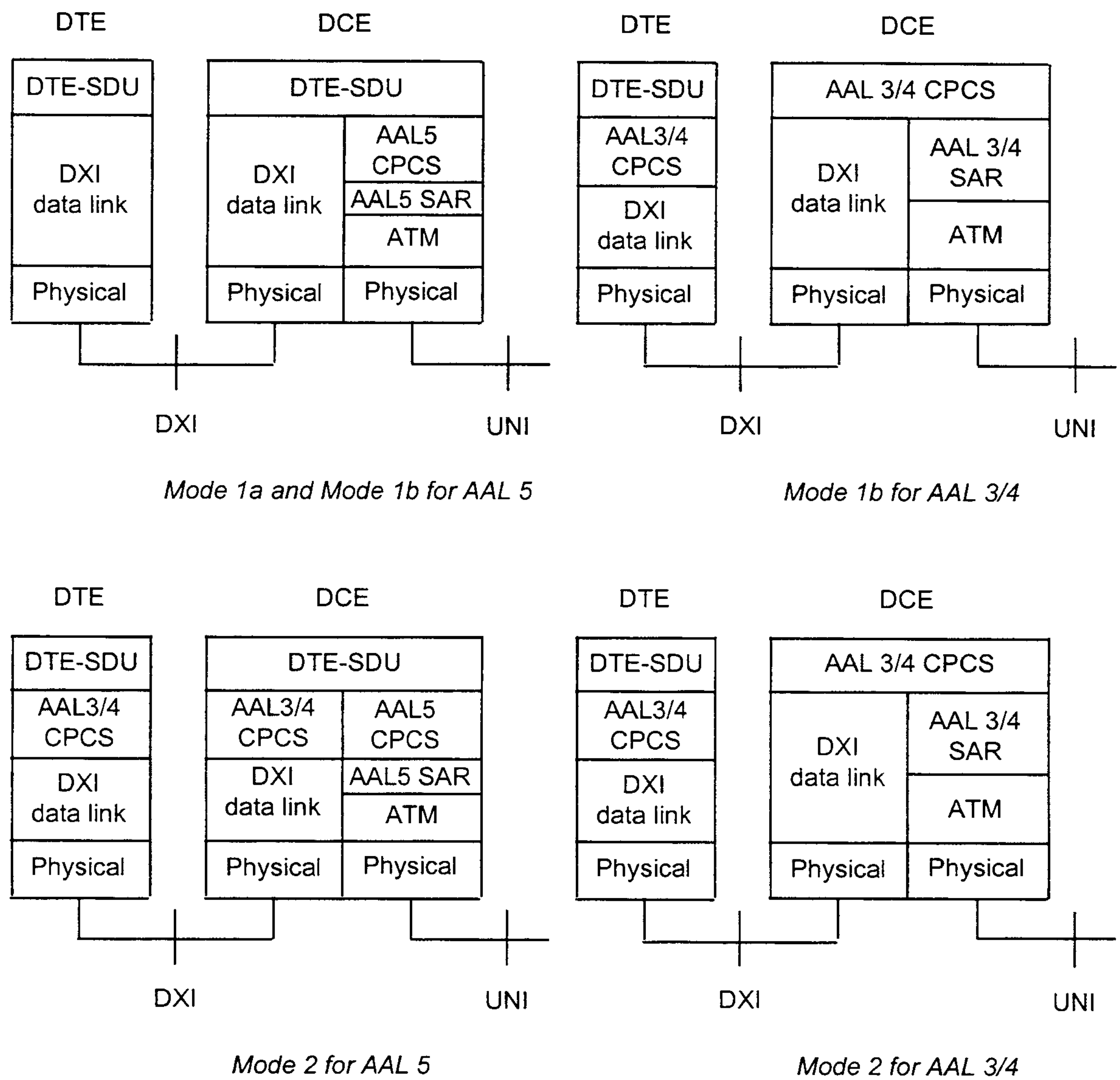


Figure 5.5: Three operational modes of a DXI

5.4 B-ICI Specification

End-to-end service across national as well as international networks may be required. Different network carriers use the B-ICI specification to communicate and to transport different services among each other. The B-ICI specifies interfaces for the physical layers, the ATM layer, and the service-specific functions above the ATM layer. The services supported by this interface are:

- Cell relay service;
- Circuit emulation service;
- Frame relay service;
- SMDS.

A service-specific non-ATM network is connected to an ATM network via an IWU.

5.5 ILMI Specification

The ILMI (Interim Local Mangement Interface) uses a prespecified ATM virtual connection to communicate (switch-to-switch) with a management application. The communication protocol is based on the simple network management protocol (SNMP). The main functions of the ILMI specification are:

- Exchange of status, configuration, and control information about link and physical layer parameters at the UNI;
- Address registration across the UNI.

The ILMI supports all physical layer interfaces defined by the ATM Forum. ILMI can manage the interfaces only between networks, but it cannot distribute management intelligence through the network.

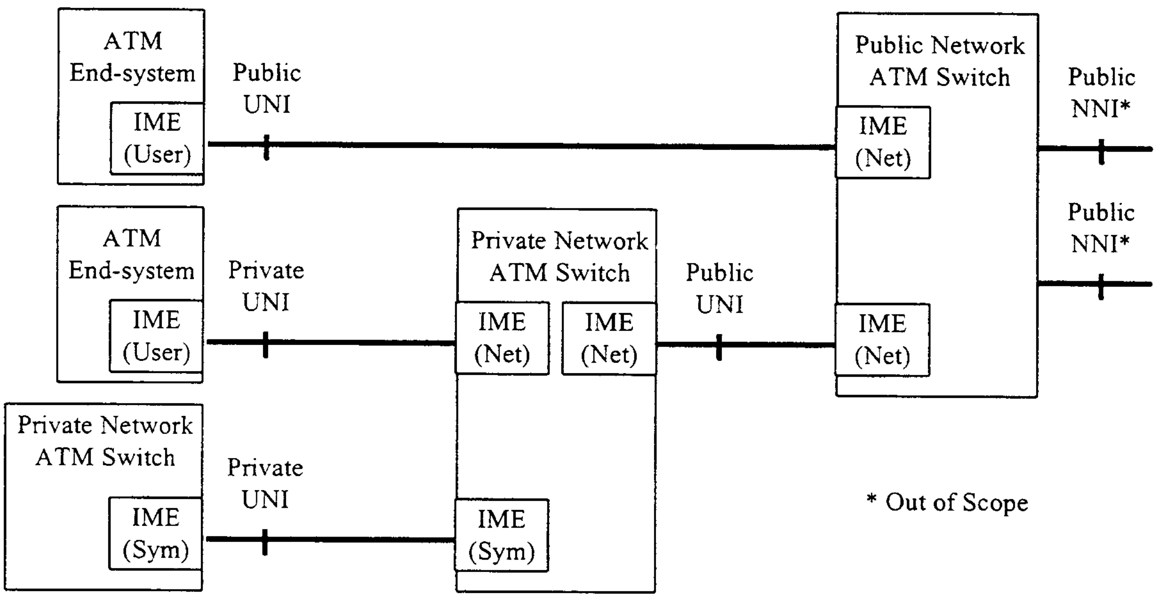


Figure 5.6: ILMI

Note: For further information about ILMI see chapter 9 and Fig. 9.3.

6 Signaling in ATM Networks

Signaling refers to the dynamic process to establish, maintain, and terminate connections between various network components. Because connections to different components are possible, four different interfaces (Private UNI, Public UNI, Private NNI, and Public NNI) are defined.

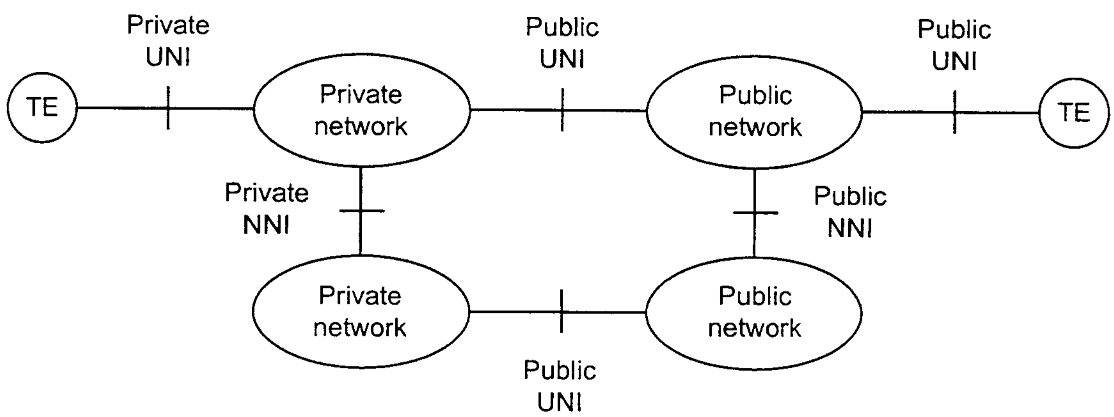


Figure 6.1: B-ISDN signaling interfaces

Signaling in private and public networks, defined in the ITU-T Q.2931B specification, is accomplished through the UNI and NNI, and is specified in the UNI 3.1 specification (ATM Forum). The signaling specification in UNI 3.1 is the newer version of the signaling protocol ITU-T Q.93B. Generally, the ITU-T focuses more on public networks, whereas the ATM Forum considers both private and public networks. Public networks are also called service provider networks. This chapter explains the signaling across the UNI, the public NNI, and the private NNI.

6.1 UNI Signaling

The capabilities for signaling between a user and a network are specified in UNI and include:

- Establishment of point-to-point VCCs;
- Establishment of point-to-multipoint VCCs;
- Tree different ATM private address formats;
- One ATM public address format;
- Symmetric and asymmetric QoS connections with a declarable QoS class;
- Symmetric and asymmetric bandwidth connections with a declarable bandwidth;
- Transport of user-to-user information;
- Support of error handling.

UNI signaling is a higher layer protocol, and runs on top of the signaling AAL (SAAL). The SAAL utilizes the AAL-5 common part (with AAL-5 SAR and AAL-5 CPCS) in addition to a service specific part consisting of two convergence sublayers:

- Service specific connection oriented protocol (SSCOP) and
- Service specific coordination function (SSCF).

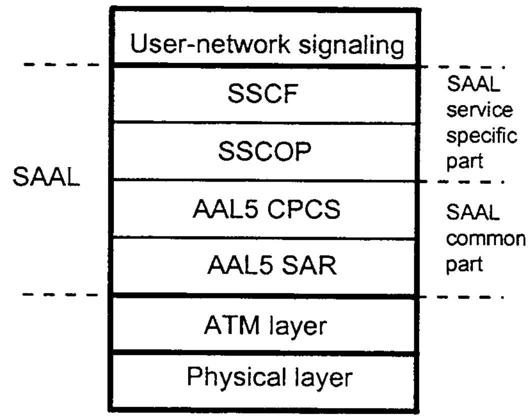


Figure 6.2: ISDN signaling structure

SSCF maps the particular requirements of UNI signaling to the requirements of the ATM layer. SSCOP provides mechanisms to establish, release, and monitor the signaling information and their exchange between peer signaling entities. The set of functions provided by the SSCOP are:

- Sequence integrity;
- Error correction by retransmission;
- Protocol control information (PCI) error detection;
- Local data retrieval;
- Connection control;
- Transfer of user data;
- Status reporting;
- Flow control;
- Keep alive.

The signaling information exchanged through the SAAL service access point (SAAL-SAP) of the UNI signaling as shown in Figure 6.3 is based on the service primitives: request, indication, response, and confirm. These signaling messages describe the traffic characteristics of the connection and its service requirements to the network.

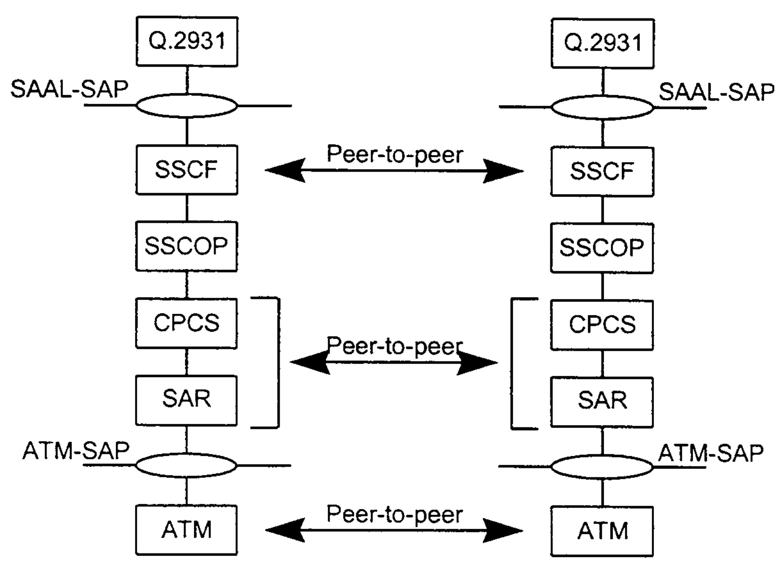


Figure 6.3: Peer-to-peer communication across the UNI

A signaling message can establish either a point-to-point bidirectional or a point-to-multipoint unidirectional connection. The categories of point-to-point call control messages are call establishment, call clearing, and maintenance signaling. A point-to-point connection is used to establish as part of a point-to-multipoint connection. Then a special message is used to add new end points or delete end users from a point-to-multipoint connection.

6.2 Private NNI Signaling

Two users, a calling user and a called user, are connected with UNIs to private networks A and B. Although each network may use its own proprietary signaling for its switches to communicate, a standardized interface, PNNI, is necessary to support interoperability between two private networks.

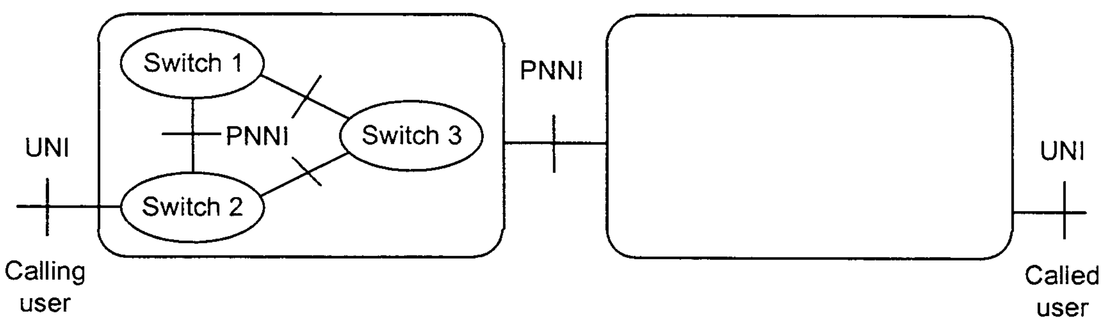


Figure 6.4: PNNI

The ATM Forum P-NNI specifies the signaling between two private networks. Since P-NNI signaling is being built on UNI signaling, most signaling messages in PNNI are the same as those of UNI. One of the major differences is that UNI signaling procedures are asymmetric, whereas those of PNNI are symmetric.

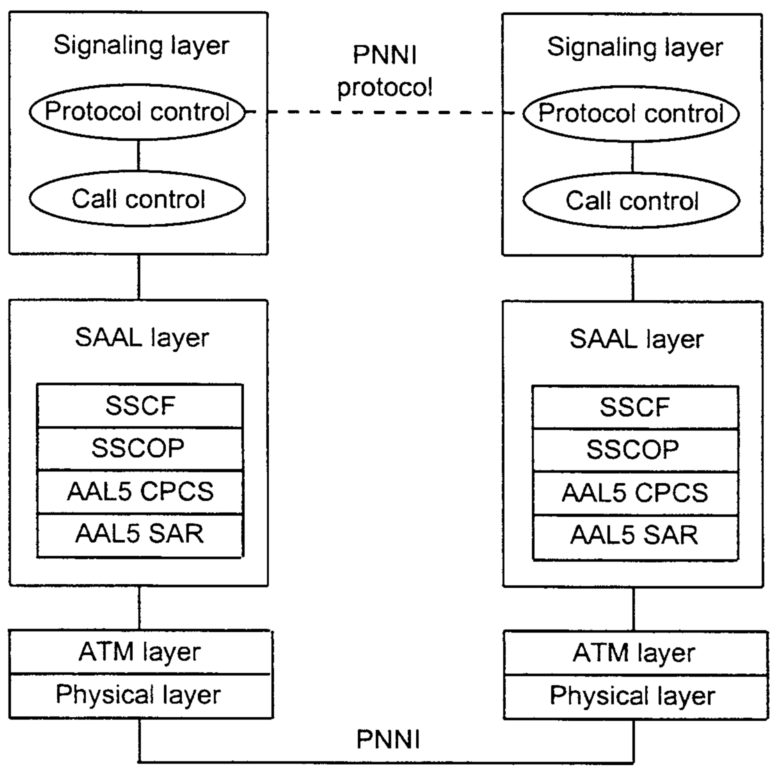


Figure 6.5: PNNI signaling structure

6.3 Public NNI Signaling

Signaling in a public network is very different from that of a private network. Typically, signaling information in a public network is carried in the same channels with user payloads. The disadvantages of this approach, called in-channel signaling, include a limited transfer rate for the signaling information exchange and a delay in establishing end-to-end connections. Consequently, in-channel signaling limits the number of types of services in the network.

6.3.1 Common Channel Signaling

Common channel signaling (CCS) was developed to solve the problems of in-channel signaling. With CCS, signaling information is exchanged over channels dedicated only for signaling. CCS is a communication architecture which was orginally designed for the transfer of signaling information between processors in communication networks. The use of CCS requires the implementation of The ITU-T Signaling System 7 (SS7). SS7 will be described later. Figure 6.6 shows a typical public network topology CCS:

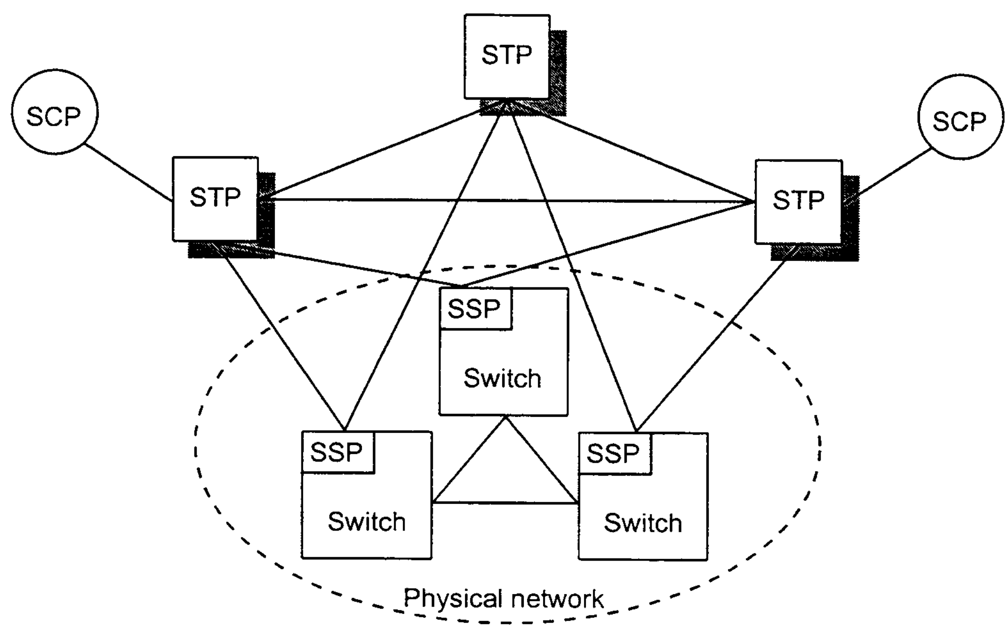


Figure 6.6: Public network with CCS

The primary components of a public network are:

- Service switching point (SSP): a network switch that contains a table and additional software-based functions;
- Service control point (SCP): a real-time processing system hosting one or more applications that provide enhanced services;
- Switched management system (SMS): a framework by which new services can be added to the network;

- Signaling transfer point (STP): an entity that transfers signaling messages from one signaling link to another;
- Intelligent peripherals (IP): a stand-alone computer that provides specific network capabilities;
- Vendor feature nodes (VFN): an off-network node connected to a service provider network.

6.3.2 SS7 Architecture

The structure of a SS7 network consists of a set of signaling points interconnected by signaling links. Signaling points are switching and processing nodes that implement the within-the-node features of SS7. With these features, two nodes can exchange signaling messages through the signaling network. A signaling mode referred to the association between the path taken by the signaling message and the signaling relation. There are three signaling modes:

- Associated mode: Messages are exchanged over a directly interconnected signaling link;
- Nonassociated mode: Messages are conveyed over two or more signaling links in tandem;
- Quasiassociated mode: A limited case of the nonassociated mode in which only certain paths can be taken for a message exchange.

SS7 is divided into a:

- Message transfer part (MTP) and
- User part.

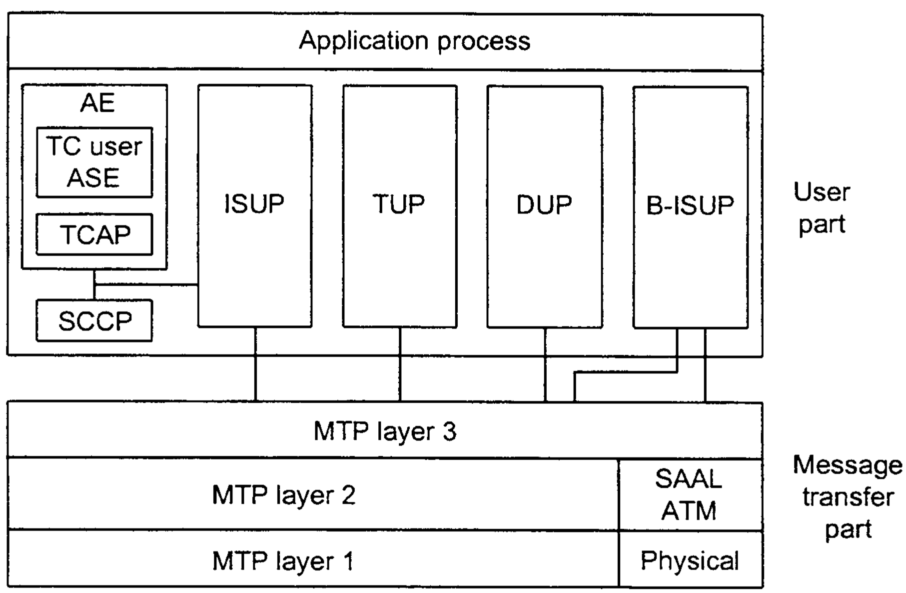


Figure 6.7: SS7 architecture

MTP works like a transport system to provide reliable transfer of signaling messages between communication user functions. The user part provides a set of functions, which can be used as transport capability by any functional entity.

SS7 functions are:

- Message transfer part (MTP);
- Signaling connection control part (SCCP);
- Telephone user part (TUP);
- Transaction capabilities (TC);
- Operations maintenance and administration part (OMAP);
- Data user part (DUP);
- ISDN user part (ISUP);
- B-ISDN user part (B-ISUP);
- Supplementary services.

The MTP consists of three layers. Layer 1 defines the physical, electrical, and functional characteristics of a signaling link. Layer 2 defines the functions and procedures for and relating to the reliable transfer of signaling messages over a single signaling data link. Layer 3 defines a set of transport functions and procedures common to and independent of the operation of signaling links. The SCCP provides a means to control logical signaling connections in an SS7 network and transfers signaling data units across the SS7 network. The TUP defines the telephone signaling functions used in SS7 for international telephone call control signaling. The TC provides a means to establish noncircuit related communication between nodes in the signaling network. The B-ISUP is the SS7 user part protocol that provides the signaling functions required to support basic bearer services and supplementary services to B-ISDN applications. It is described in more detail in the next section. The application process provides a set of functions and features to support a particular network requirement. The application elements (AE) represent the communication functions of the application processes.

6.3.3 B-ISDN User Part

The B-ISDN user part (B-ISUP) is being developed for international applications as an NNI. It is a set of functional blocks, each representing a particular function. B-ISUP uses the elements of signaling information described in the Recommendation Q.2762 to support B-ISDN applications. Its features include the following:

- Demand (switch virtual) channel connections;
- Point-to-point switched channel connections;
- Connections with symmetric or asymmetric bandwidth requirements;
- Single connection (point-to-point) call;
- Basic signaling functions via protocol messages, IEs and procedures;
- Class X, class A, and class C ATM transport services;
- Request indication of signaling parameter;

- VCI negotiation;
- Out-of-band signaling for all signaling messages;
- Error recovery;
- Public UNI addressing formats for unique identification of ATM end points;
- End-to-end compatibility parameter identification;
- Signaling interworking with ISDN and provision of ISDN services.

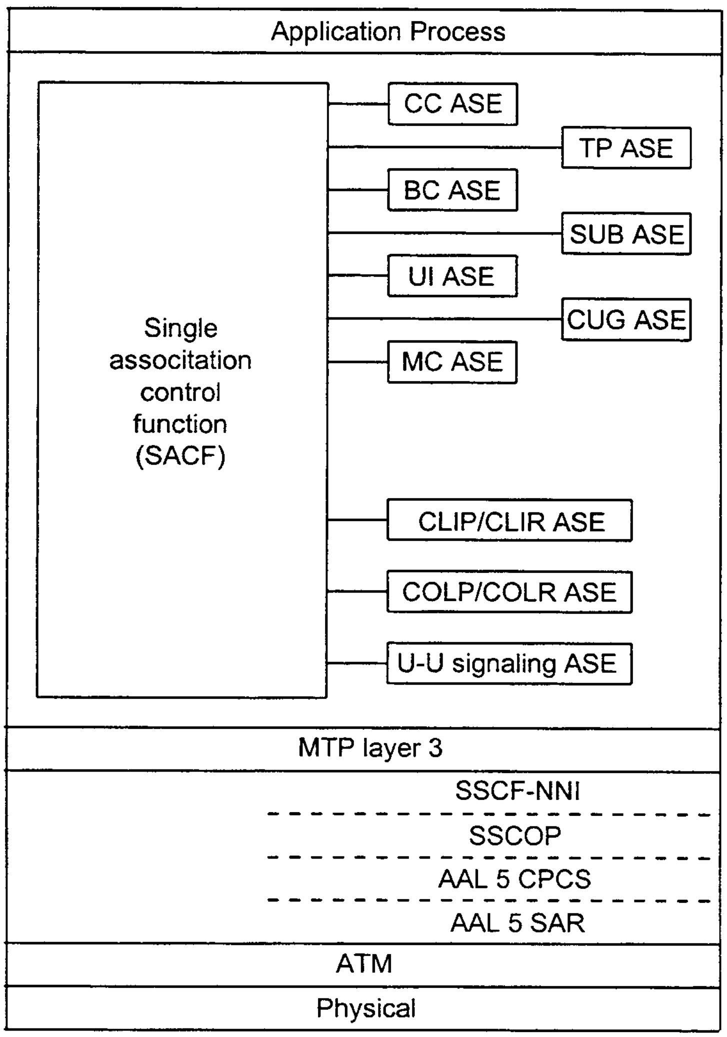


Figure 6.8: B-ISUP specification model

ASE: application service element

CC: call control

BC: bearer control

SUB: subaddressing

UI: unrecognized information

CUG: closed user group

MC: maintenance

CLIP: calling line identification presentation

CLIR: calling line identification restriction

COLP: connected line identification presentation

U-U: user to user

7 Routing

7.1 General Discussion

A network consists of many devices and nodes interlinked by connections. If no direct connections between these devices exist, the network has to route the traffic until it is delivered to the destination. A routing function, the process of selecting a path between traffic source and destination, should possess the following attributes:

- Correctness;
- Simplicity;
- Robustness;
- Stability;
- Fairness;
- Reliability.

The routing algorithms used in existing packet-switched networks are generally variants of the shortest path algorithms. Routing techniques differ depending on the time and place where routing decisions are made, and may vary in different networks. The time when a decision is made refers to whether the routing decision is made at the packet level or the virtual-circuit level. The place where a decision is made refers to whether it is made through distributed routing, centralized routing, or source routing. The time and place where routing decisions are made determine the amount of routing information that needed to be exchanged.

7.2 Routing in ATM Networks

In an ATM network, which is connection-oriented, routing decision is made at the virtual circuit level; that is, the transmission path joining the source and destination(s) of a virtual circuit is determined before user traffic is transferred. There are two hierarchies of virtual connections: virtual path connections (VPCs) and virtual channel connections (VCCs). The goal of having two hierarchies of connections is to simplify switching and offer flexibility. A number of VCCs may be multiplexed onto a VP and a group of VPs may, in turn, multiplexed onto a physical transmission link. Two identifiers, virtual path identifier (VPI) and virtual channel identifier (VCI), are needed to uniquely determine a particular VCC. One is to specify the VP to which the VCC belongs, and the other is to specify which of the VCCs within the VP is the VCC in question. The VPI and VCI of a cell, along with the physical transmission link from which the cell is received by an ATM switch, uniquely determine the next outgoing link of the cell.

One of the advantages of using an ATM network is the flexible bandwidth allocation that it offers, but the dynamic allocation of bandwidth poses difficulties on a routing function. For example, the initial equivalent bandwidth allocated to a VP cannot be maintained if there were failures in the network. Indeed, an ATM routing function, aside from selecting an appropriate path for a virtual connection, must also perform the following tasks to mitigate the effect of network failures and the inherent variability of traffic load:

- Fast changes to the allocated bandwidth of a VC/VP;
- Quick detection of failures and fast rerouting of VCs and VPs that were using failed components;

- Flexible means of adding and deleting VPs to adjust to the variability of traffic over different time frames.

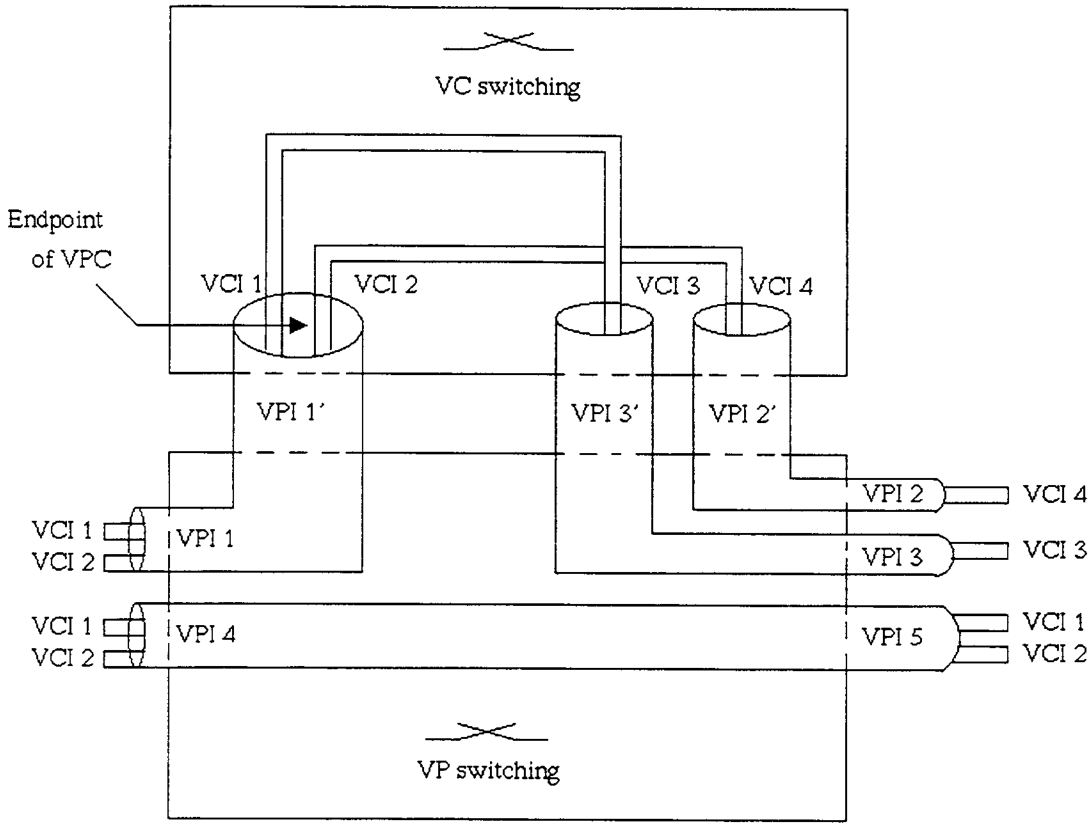


Figure 7.1: VC and VP switching

The particular routing technique used typically depends on whether the network is public or private. The following routing methodologies are used in public ATM networks:

- ❒ Shortest path routing;
- ❒ Fixed-path routing;
- ❒ Saturation routing;
- ❒ Stochastic learning automata-based routing;
- ❒ Routing in telephony networks: e.g., Dynamic Nonhierarchial Routing (DNHR) or Dynamically Controlled Routing (DCR).

For private ATM networks, the ATM Forum PNNI specifications define what routing information is used and how it is disseminated among ATM switches. No routing protocols have been specified. The specifications provide a standard-based framework for PNNI signaling and routing. The main function of PNNI routing is to find a path across a network between end stations in a point-to-point or point-to-multipoint connection.

Based on this framework, PNNI routing requires:

- Unique identification of switching systems and the PNNI links connecting them;
- The availability of the topological information on the PNNI network at switching systems;
- Path selection algorithm;
- Connection admission control (CAC) procedure.

Figure 7.2 illustrates the relationship among the essential components in PNNI routing.

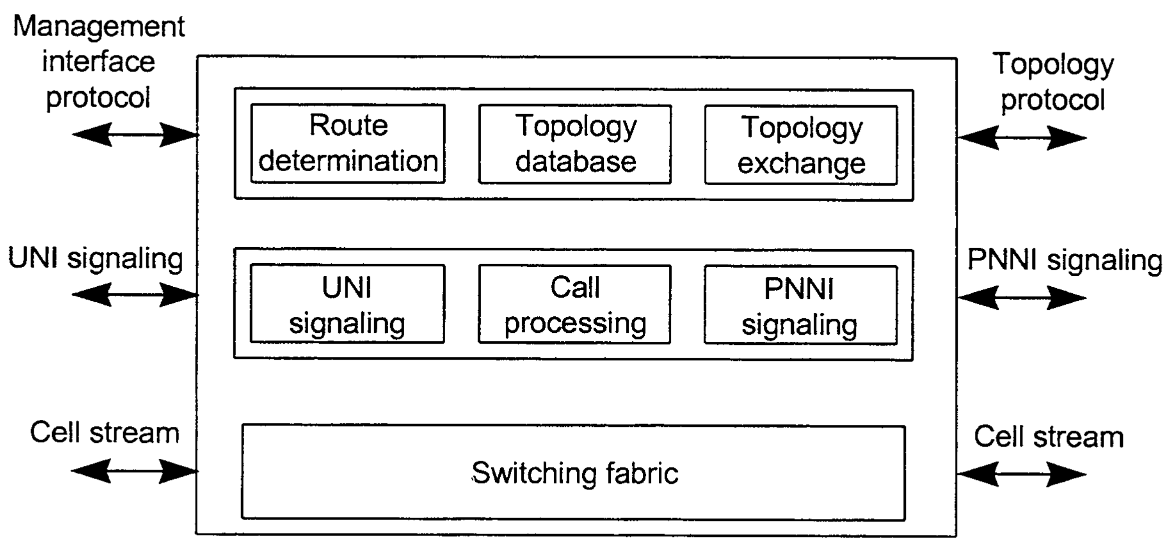


Figure 7.2: PNNI framework

8 Transport Protocols

8.1 General Discussion

The primary function of a transport protocol is to establish, manage, and terminate a connection and to provide services needed by the higher layers. The functionalities required by communicating B-ISDN applications can be summarized as follows:

- Throughput;
- Delay;
- Error tolerance;
- Real-time versus non-real-time;
- Isochronism;
- Connection-oriented versus connectionless;
- Error detection, correction or recovery;
- Acknowledgement and flow control;
- Synchronization of various types of data services.

The nine functional requirements suggest that nine classes of transport protocols can be defined. The most important features of transport protocols are:

- Signaling;
- Handshake;
- Connection parameters;
- Multiplexing;
- Acknowledgement;
- Flow control techniques;
- Error handling;
- Evaluation of features.

Various transport protocols exist and are used in standardized commercial networks. The most well-known transport protocols are:

- ❒ TCP: CO, three-way handshaking, PAR for acknowledgement;
- ❒ ISO/TP4: CO, three-way handshaking, PAR.

In addition to these two protocols, many so called lightweight protocols exist. They are developed to minimize the overhead, and are used primarily in high-speed networks:

- ❒ Delta-T;
- ❒ UPR (universal receiver protocol, datakit);
- ❒ NETBLT (network block-transfer protocol);
- ❒ VMTP (versatile message transaction protocol);
- ❒ Advanced peer-to-peer networking;

- ❒ RTP (rapid transport protocol);
- ❒ XTP (Xpress transfer protocol).

Although ATM can support these protocols and offer interfaces for them. ATM may require a different set of transport protocols in order to support the high-speed transfer of real-time data, video, and voice.

8.2 Real-Time Protocols

Real-time applications such as voice and video typically have very stringent delay and jitter requirements. Traditionally, they are supported by circuit-switched networks, which introduce very small latency and jitter to their traffic. Since traffic typically arrives to its destination within the latency and jitter requirements specified, a real-time application does not need additional adaptations. A packet-switched network, because its resources are statistically shared, can introduce potentially large latency and jitter that are not acceptable by a real-time application; consequently, special adaptations are required to compensate or control the latency and jitter introduced. These adaptations can be implemented in an application, an ATM adaptation layer (if the network and application are entirely ATM-based), or a layer in between the application and the subnetwork. The entity that provides adaptation functionalities between an application and an subnetwork is generally referred to as a transport protocol. A transport protocol should provide the following functionalities:

- Transmission of media streams over any network connection;
- Support of different payload types;
- Provide information needed to synchronize various streams;
- Flow & congestion control (consumed bandwidth);
- Efficiency in usage and implementation;
- Packet source tracing after arrival;
- Reliability (correct reproduction of the sent stream).

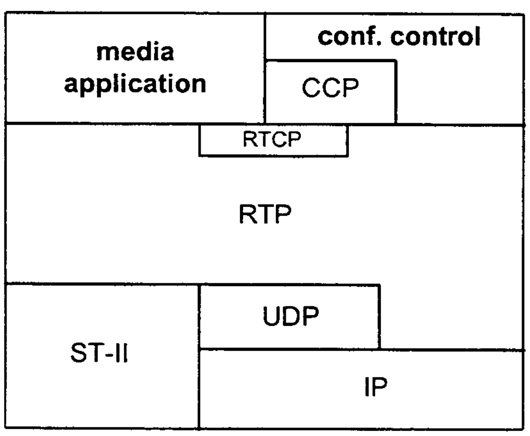


Figure 8.1: RTP environment

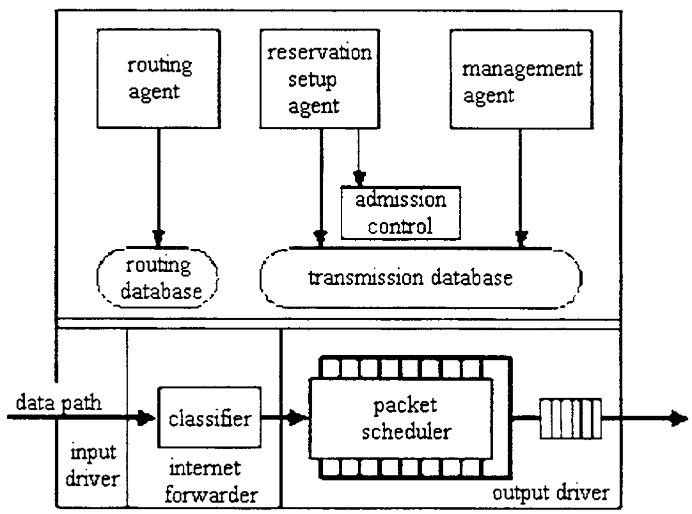
The Real-time Transport Protocol (RTP), developed by the Audio-Video Transport Group of the IETF, is one such real-time transport protocol. It is specified by the IETF in RFC 1889 for voice and in RFC 1890 for video transmission. RTP is designed independent from structure of the subnetwork, and, therefore, can be used either with ATM, IP, or IPv6. If RTP is used in an ATM environment, it would run on top of AAL-5; in an IP environment, UDP; and in IPv6, ST-II (Figure 8.1).

The Real-Time Control Protocol (RTCP), an integral part of the RTP, was developed to control the data streams between receiver and transmitter. The RTCP data stream is uncertain. The users send status information periodically. The four roles of the RTCP are:

1) To furnish information on the quality of data distribution;
2) To keep track of all participants in the real-time session with the help of the transport-level RTP source indentifier, called canonical name (CNAME), and the synchronization source identifier (SSRC);
3) To control the rate of the RTCP packets which are transmitted by the participants;
4) To identify the source and the format of the data streams.

The Resource Reservation Protocol (RSVP) was developed by the IETF to support the network manager for the administration of real-time applications in a packet-switched multicast environment. The main features of RSVP are:

- Suppport for heterogeneous service needs;
- Flexible control over the way reservations are shared along branches of multicast delivery trees;
- Scalability to large multicast groups;
- Ability to preempt resources to accomommodate advance reservations.



Every node on a transmission path reserves the requested resources for a connection. The admission control checks if enough resources are available. RSVP can be used in a unicast and a multicast connection. Every receiver can make a request for a specified quality of service. The classifier assigns each packet a priority and classifies the sequence using stored reservation tables. RSVP can be used with IPv4 or IPv6.

Figure 8.2: RSVP-router

Each traffic stream within a multimedia session is carried in a separate RTP session (Figure 8.3). Every session has its own RTCP to maintain the required QoS in the data stream. The routers communicate via the RSVP to set up and manage the bandwidth allocation.

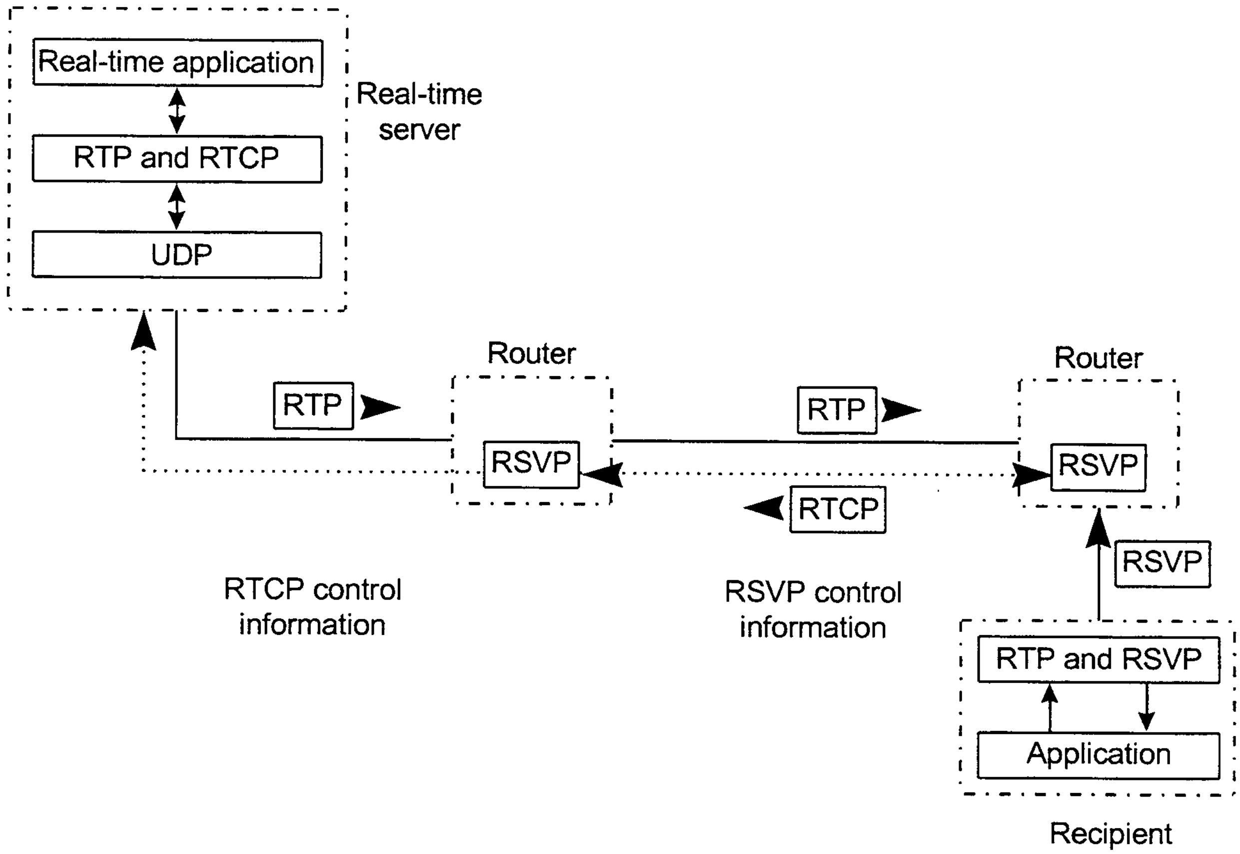


Figure 8.3: Protocols in a multimedia session

9 ATM Network Management

9.1 General Discussion

As the complexity and size of communication networks increase, network administration functions are increasingly mechanized and usually performed by an automatic network management consisting of:

- ❐ Management station or manager;
- ❐ Agent;
- ❐ MIB;
- ❐ Network management protocol.

Most of the existing network management systems are based on the OSI network management model.

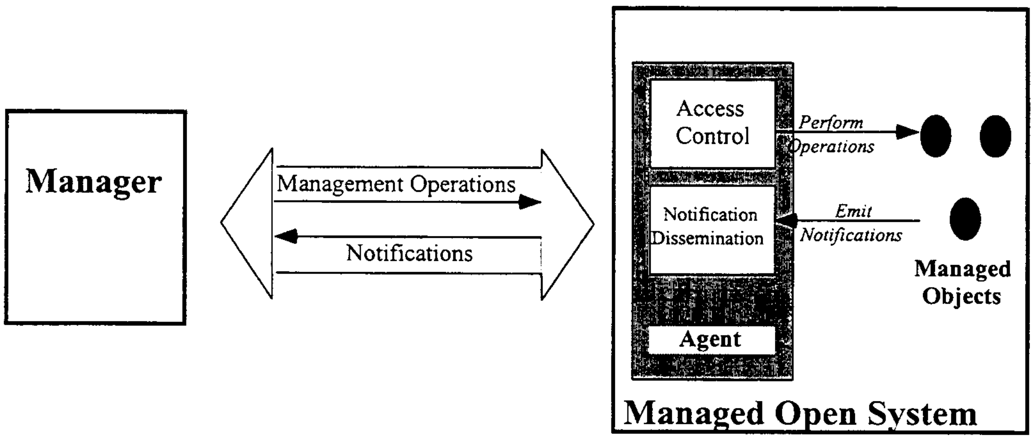


Figure 9.1: OSI network management model

The functionalities provided by network management are defined by the ISO as:

- Configuration management: The facilities that exercise control over, identify, collect data from and provide data to managed objects for the purpose of providing continuous operation of interconnection services;
- Fault management: The facilities that enable the detection, isolation, and correction of abnormal operation of network resources;
- Performance management: The facilities needed to evaluate the behavior of managed objects and the effectiveness of communication activities;
- Security management: Addresses those aspects essential to operate network management system correctly and to protect managed objects;
- Accounting management: The facilities that enable charges to be established for the use of managed objects and costs to be identified for the use of those managed objects.

The ATM network management system is based on the Telecommunication Management Network (TMN) Model specified by ITU-T M.3010.

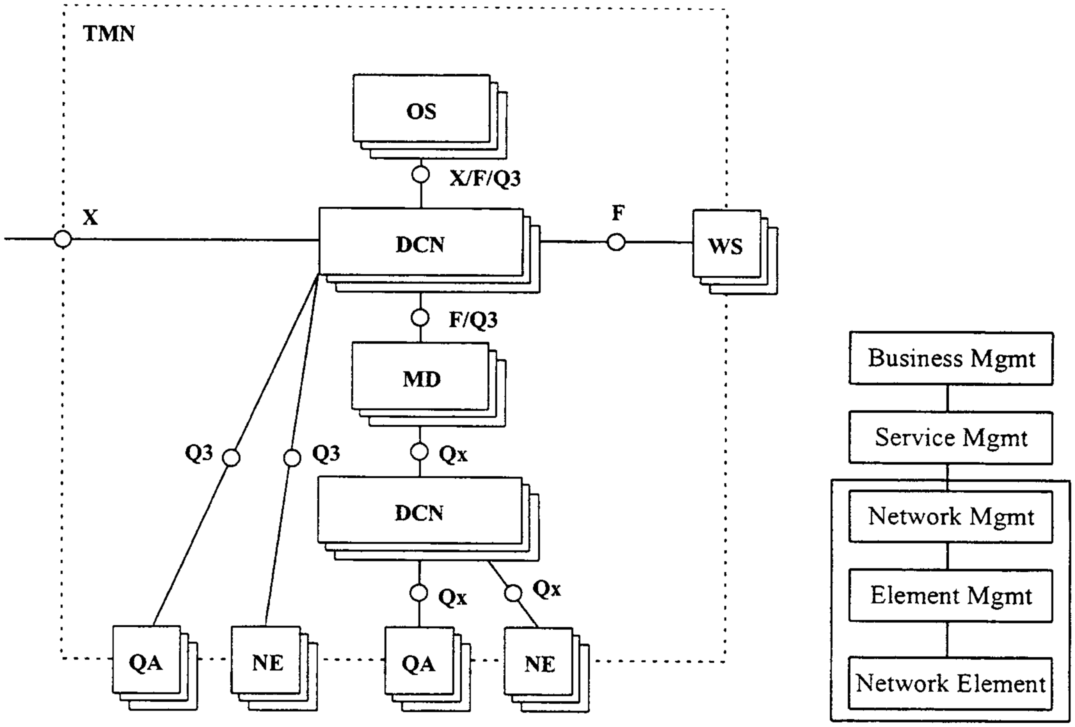


Figure 9.2: TMN model

Most of the ATM network management is based on already existing standards, e.g., SNMP (simple network management protocol) and CMIP (common management information protocol).

9.2 Network Management Protocols

Network management is performed through the communication between a manager and several agents as prescribed by a manager/agent model (Fig. 9.1). The manager controls the network management. An agent controls the managed objects and adjusts them as directed by its manager. A communication protocol is necessary to handle the information exchange between a manager and the agents. The management protocol should provide the following functions:

- Reading and updating attributes of managed objects;
- Requiring managed objects to perform a specific function;
- Reporting results produced by managed objects;
- Creating and deleting managed objects.

The two most important standard management protocols are SNMP and CMIP.

The connectionless SNMP was developed by the IETF in the late 80's to handle data communications and to manage TCP/IP networks. SNMP is an application layer protocol that utilizes the user datagram protocol (UDP), which does not provide reliable transfer, at the transport layer. The unreliable information exchange and the limited security features are the major disadvantage of SNMP Version 1 (SNMPv1). SNMP version 1 (SNMPv1) is defined in RFC 1157. The backward compatible SNMPv2 (specified in RFC 1901-1908) offers more security and fixes to SMI (Structure of Management Information). SNMPv3 should be available in 1997/98. It has an improved modularization and administration with remote configuration and key management. The connection-oriented Common Management Information Protocol (CMIP) was developed by the ISO. It is more powerful and complex than the SNMP. The specification ITU-T X.711 (equivalent to ISO 9596) describes how to use CMIP with LME (layer management entity) and SAME (system management application entity) within ISO frameworks.

9.3 SMI and MIB

The most important part of a management system is the management information at the agents because all the network management decisions are based on it. In the past, much effort has been spent on the definition and the standardization of this information. A management information specification language, called SMI (Structure of Mangement Information), is used for the exchange of this information. SMI is defined in RFC 1155 and is later enhanced with the addition of a trap macro in RFC 1215. The MIB (Management Information Base) standards define the network management variables and their meanings (e.g., RFC 1213 or RFC 1573). Different MIBs exist for different network types (e.g., FDDI, 802.5, ATM). The ATM Forum has defined MIBs for the following ATM interfaces:

- UNI;
- DXI;
- B-ICI;
- LUNI (LAN Emulation UNI).

9.4 ATM Network Management

The network management for an ATM network looks similar to that of other networks. The reason is that the ATM Forum has been developing a five-layer ATM network management reference model based on the TMN model. Parts of the ATM management model are:

- ❒ Five different interfaces (M1 to M5): for managing hybrid network environments that consist of both privat and public networks and extend from LAN to WAN;
- ❒ The ILMI (described a few chapters earlier) and an
- ❒ OAM facility.

The functions of the five defined management interfaces (M1 to M5) in this reference model (Fig. 9.3) are:

- ❒ M1: supports various functions for the management of the ATM devices;
- ❒ M2: supports functions for the management of private ATM networks;
- ❒ M3: allows the two management systems (one in a private network and the other in a public network) to communicate to each other;
- ❒ M4: supports functions for the management of public ATM networks;

❒ M5: provides communication capabilities between two management systems of public networks.

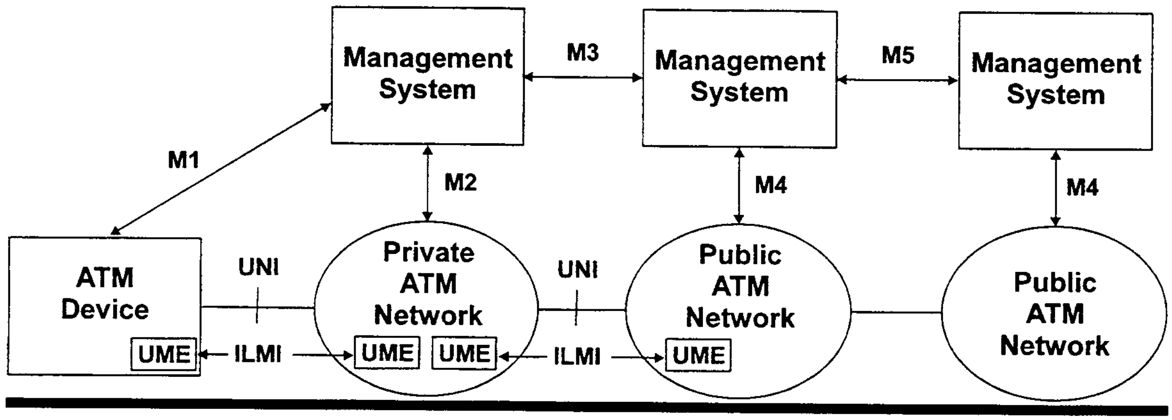


Figure 9.3: ATM management model

Interfaces M1 to M5 will support the five network management functions (configuration, fault, performance, security and accounting management). M1 and M2 can be used for private network management. M1 and M2 include SNMP-based specifications defined by the IETF, which are known as AToM MIBs (the "o" in "AToM" signifies SONET). The AToM MIBs describe how to configure a network and how to address various AALs and switch-related management. The current AToM MIB (RFC 1695) uses the SNMPv2 (RFC 1573) and defines the information for managing ATM devices within an ATM network or cross-connect nodes that include:

- ATM interface configuration group;
- DS3 interface group;
- Transmission convergence sublayer group;
- ATM traffic parameter group;
- ATM VP link group;
- ATM VC link group;
- ATM VP cross-connect group;
- ATM VC cross-connect group;
- AAL5 group.

M3, the Customer Network Management (CNM) interface, is a SNMP-based interface and is defined in two classes. Class I provides monitoring information, whereas Class II has monitoring and controlling features. Most of the M3 management features are based on IETF MIBs (RFC 1213, 1406, 1407, 1573, 1695).

M4 is the management interface to enable Network Management Level (NML) views and Element Management Level (EML) views to the carrier's network management system and the public ATM network. Figure 9.5 illustrates the association between the network and the Network Elements (NEs). The current M4 interface requirements are defined in the following areas of ATM network management:

- Network configuration management;
- Network fault management;
- Network connection configuration management;
- Network connection fault management;
- Network connection monitoring management;
- Internetwork link management;
- Network planning and performance management.

M5 is the management interface between carriers' own network management systems. The ATM Forum Network Management Working Group is working on the customer requirements for the interface. M5 is the most complicated of the five interfaces.

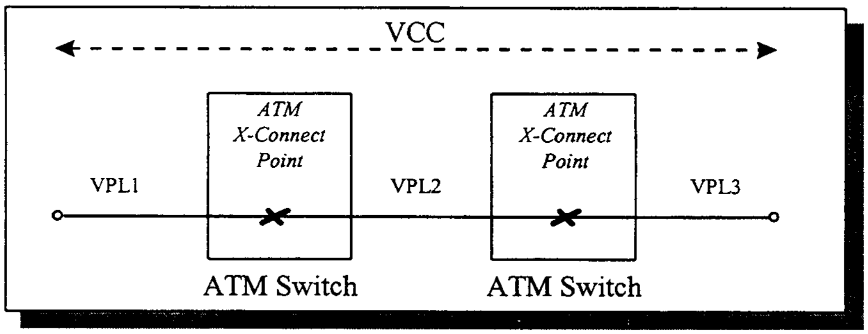


Figure 9.4: Private network management: M1, M2

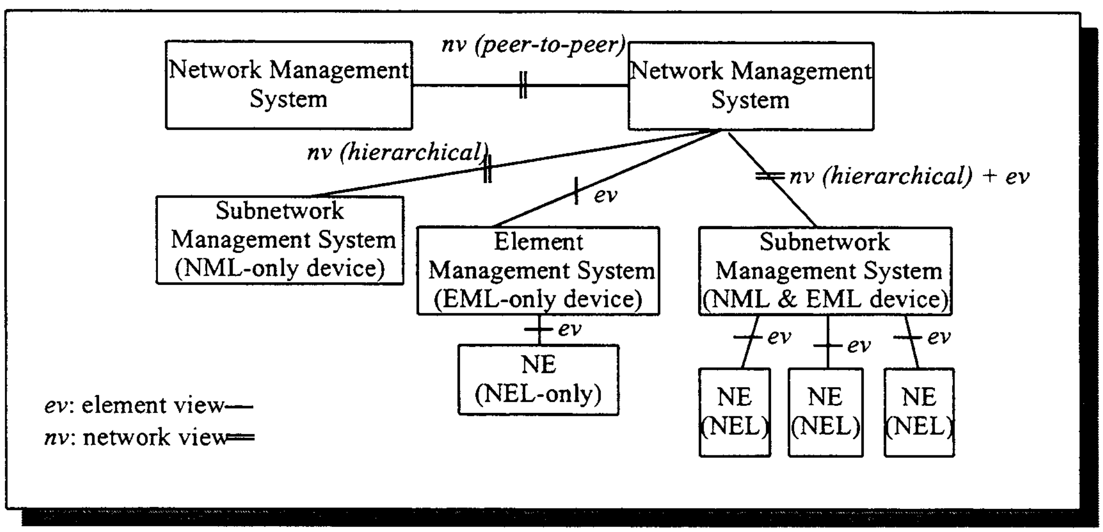


Figure 9.5: M4 network and network element views

10 Applications

10.1 Non-real-time Applications

Many of the current data communications infrastructures are based on a LAN architecture. The success of ATM may depend on its ability to support existing LAN applications. Since the ATM technology is very different from a traditional LAN architecture, integrating LAN applications with ATM poses many usual challenges. This chapter describes how to run non-ATM applications based on older data protocol standards over an ATM network.

10.1.1 Frame Relay Internetworking with ATM

Several connection standards exist for a net manager to run frame relay traffic across an ATM backbone net or simply connect Frame Relay and ATM networks directy. These schemes are:

- Frame Relay/ATM network interworking;
- Frame Relay/ATM service interworking and
- FUNI (frame-based user-to-network interface).

An interworking between Frame-Relay and ATM can be achieved through either Networking-Interworking or Service-Interworking. Network-Interworking is possible with a Frame-Relay Emulation (FR-SSCS) software running on an ATM end-system. The Frame Relay Forum defined the specification FRF.5 for Network-Interworking. Service-Interworking involves an intermediate interworking function to provide mapping between the Frame Relay Protocol (Q.922) and AAL5 (I.363). This approach relies on protocol conversion instead of tunneling Frame Relay traffic across the ATM net. Frame Relay and ATM use different IP encapsulation techniques to support the IP traffic in the case of Service-Interworking. Frame Relay uses RFC 1490 and ATM uses RFC 1483. The ITU-T has defined this specification in Recommendations I.55 and I.365.1. The Frame Relay Forum FRF.8 defines the Service-Interworking. FUNI, although not as common as the other two approaches, is a means to allow a cost effective access to all devices in an ATM WAN through the use of a frame-based format. FUNI shares a common signaling protocol with the ATM UNI, and permits a PVC setup in a relatively simple way. The Frame Relay Forum and the ATM Forum are working to reduce the complexity in the interworking of the two technologies. For example, the Frame Relay Forum has defined FRF.10 to specify SVC signaling over an NNI.

10.1.2 SMDS Service over ATM

Switched Multimegabit Data Service (SMDS) is a packet-switched public data service, and provides a LAN-like transport across MANs and WANs. It supports QoS, maximum packet size, and uses the E.164 addressing format. SMDS is a carrier service. The ITU-T Recommendations F.812, I.211, I.327, I.362, I.363, and I.364 describe how to provide interworking service between current SMDS and B-ISDN or ATM connectionless packet service. There are two general approaches to provide the connectionless service in B-ISDN:

- Direct service and
- Indirect service.

The indirect service approach is the easier way to provide connectionless service by terminating connectionless protocols at the edges of the ATM network through the use of IWUs (see Fig. 10.1).

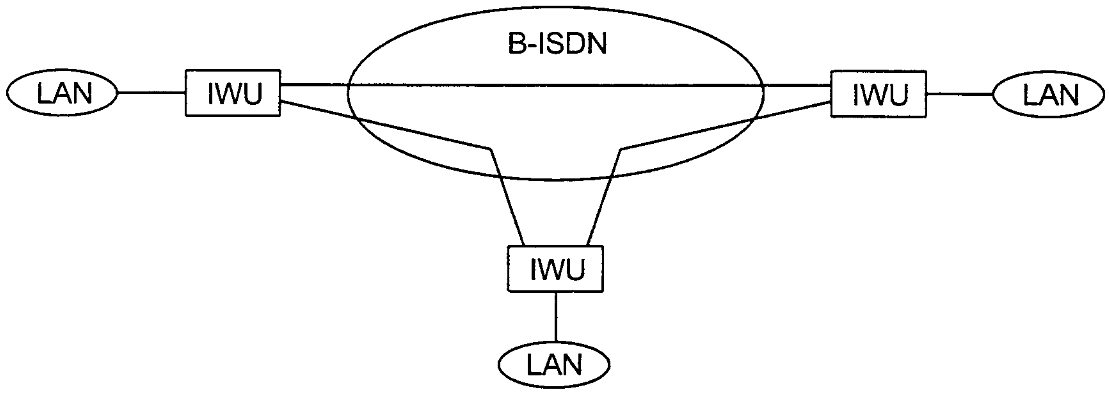


Figure 10.1: Indirect connectionless service

In the direct approach, the connectionless service function (CLSF) is provided through the use of connectionless server (CLS):

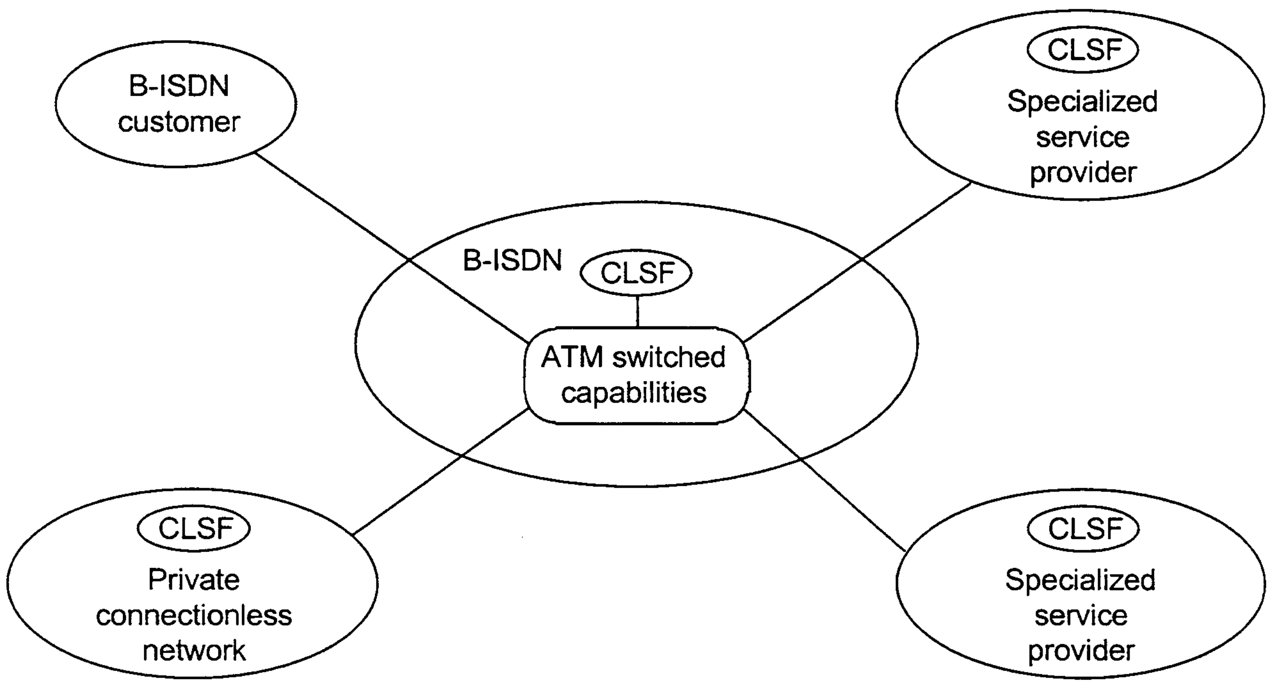


Figure 10.2: Connectionless service function configuration

The CLS supports the connectionless service function and ATM interfaces. The connectionless network interface protocol (CLNIP) is used for transmission of LAN frames. The connectionless service to an ATM network is supported by using an AAL3/4 and the connectionless network access protocol (CLNAP). The CLS provides addressing and routing of connectionless frames and adaptation to the connectionless protocol. The general protocol structure for connectionless data service in B-ISDN is illustrated in the Figure 10.3:

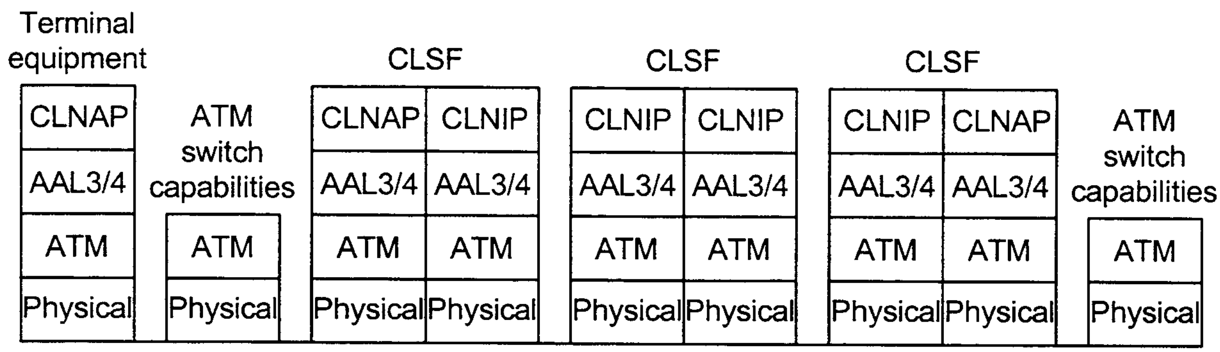


Figure 10.3: Protocol structure for connectionless data service

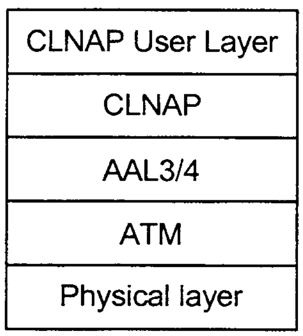


Figure 10.4: Connectionless layer service

CLNAP provides connectionless layer services, which include routing, addressing, and QoS selection. The CLNAP layer uses the AAL service and provides it to the CLNAP user layer (Fig. 10.4).

As mentioned before, these proposals use the AAL3/4, whereas other connectionless services, to be described next, are based on AAL5 services.

10.1.3 IP over ATM

Because of the fact that IP-structures are widely used, it is important for both IP and ATM networks to interwork. Solutions to realize IP over ATM without modifying existing IP applications have been researched and found:

- Multiprotocol Encapsulation over ATM Adaptation Layer 5 (IETF RFC 1483);
- Classical IP and ARP over ATM (IETF RFC 1577);
- LAN Emulation (ATM Forum LANE.v1).

Which of the solutions performs the best is still a subject of debate, and will largely depend on the particular implementation of each respective solution. The differences between these solutions are only in the data link and the network layer (Figure 10.5).

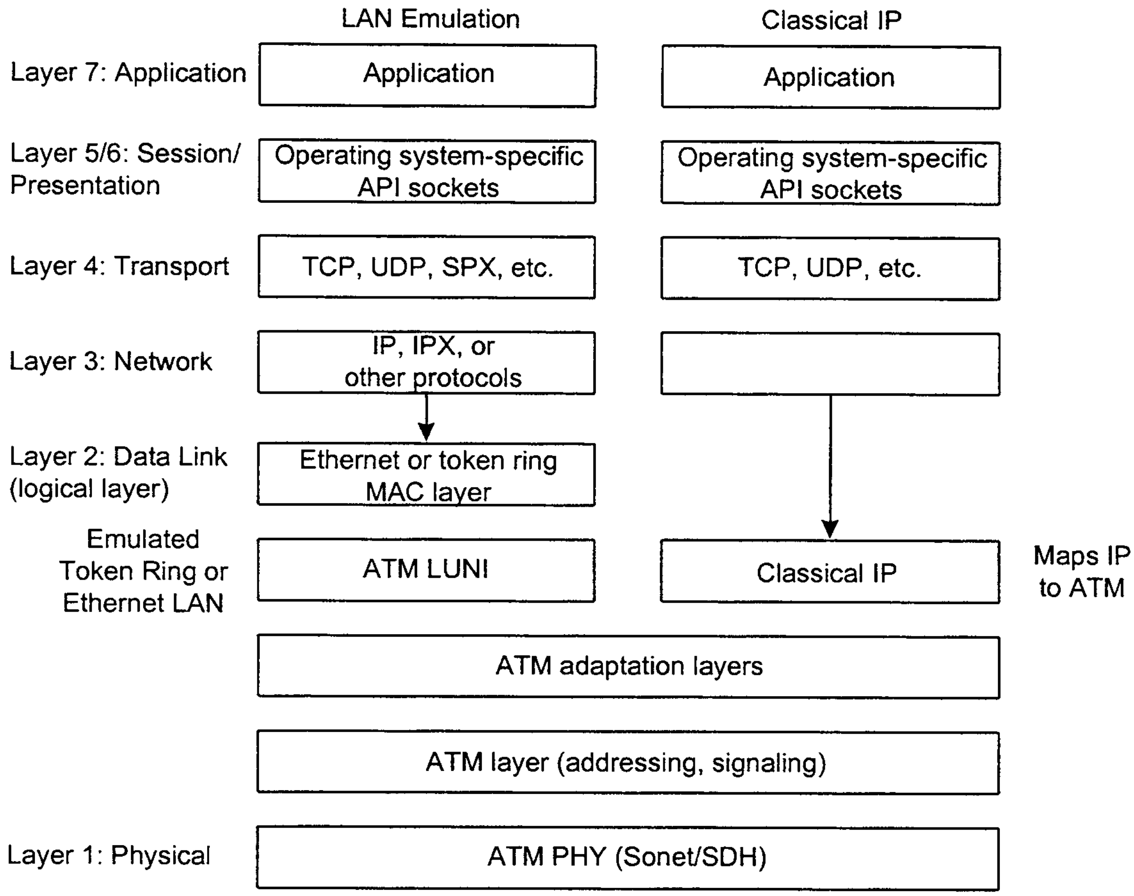


Figure 10.5: IP over ATM

RFC 1483 describes two encapsulation methods for carrying network interconnect traffic accross an ATM network using AAL5. The first method, called LLC Encapsulation, allows multiplexing of multiple protocols (e.g., IP, IPX) over a single ATM virtual circuit. The second method, called VC Based Multiplexing, assumes that each protocol is carried over a separate ATM virtual circuit.

RFC 1577 defines an initial application of classical IP and ARP (address resolution protocol) in an ATM network environment configured as a Logical IP subnet (LIS). It is a straightforward protocol that runs over ATM permanent virual circuits (PVCs) and switched virtual circuits (SVCs). RFC 1577 supports IP subnets and allows net managers to define ATM QoS features on a subnet-by-subnet basis. Only operations within each logical IP subnet (LIS) are defined. This approach is common in networks connecting workstations.

ATM Forum LANE (LAN Emulation) offers another means to support IP applications over ATM. It emulates a LAN such as an Ethernet or a token ring. Working like a bridging protocol at layer 2 of the OSI model, LANE does not emulate all of the actual MAC protocols, e.g., CSMA/CD for Ethernet or token passing for token ring. LANE works as interworking service over AAL5. LANE for FDDI has not been defined yet. In order to support FDDI applications, it is necessary to convert the FDDI packets into Ethernet or a token ring format before utilizing the LANE service.

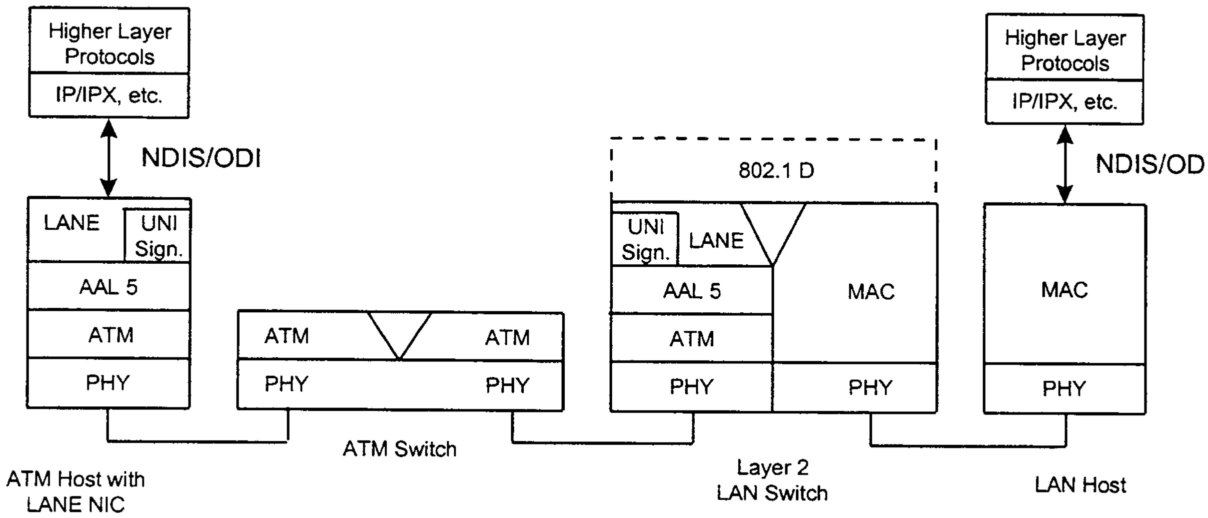


Figure 10.6: LANE Protocol Architecture

LANE is used primarily for the following applications:

- Centralizing servers and using ATM adapters to attach them directly to an ATM network;
- Integrating existing LANs over an ATM transport backbone.

LANE follows a client/server model, with multiple clients connecting to LANE components. These clients, called LAN Emulation Clients (LECs), are located in each host, one for every ELAN that the host wishes to be attached.

The LANE components are:

- Broadcast and Unknown Server (BUS);
- LAN Emulation Server (LES);
- LAN Emulation Configuration Server (LECS).

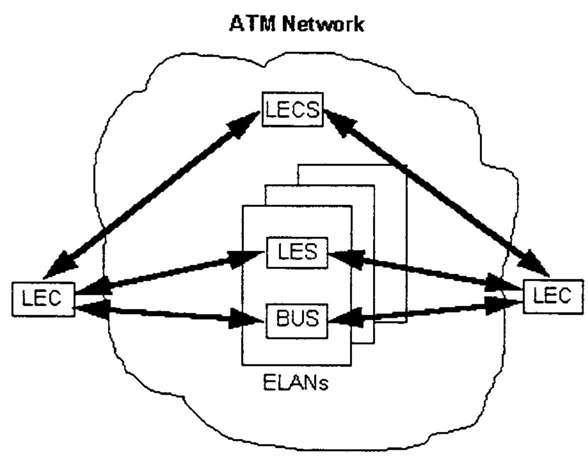


Figure 10.7: ATM Forum LANE Model

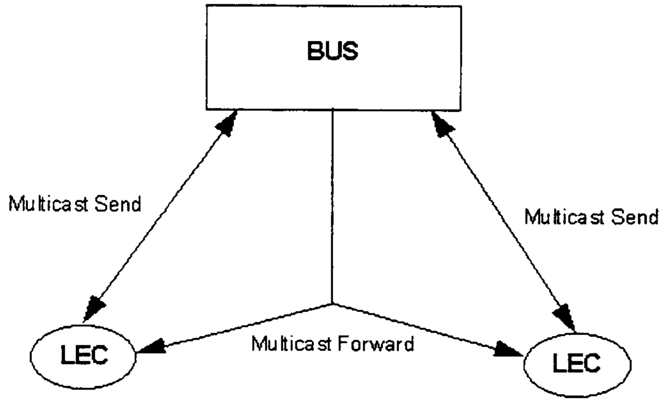


Figure 10.8: BUS (Broadcast and Unknown Server)

BUS is the multicast server for an ELAN with one logical BUS per ELAN. If the BUS receives a Multicast Send message from a point-to-point connected LEC, it will forward this message (Multicast Forward) in a point-to-multipoint connection to all LECs.

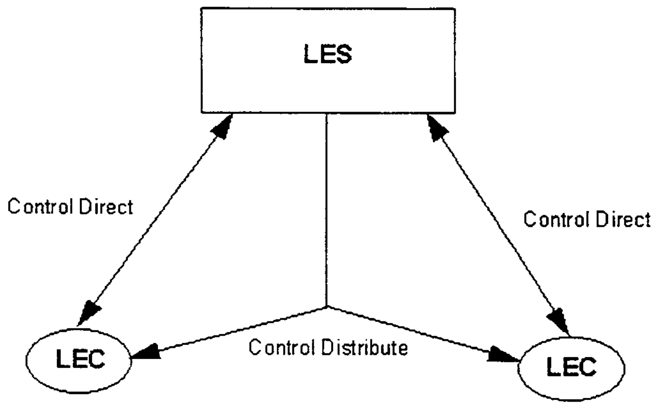


Figure 10.9: LES (LAN Emulation Server)

LES is the address resolution server for an ELAN with one logical LES per ELAN. It maps LAN MAC addresses to ATM addresses. If the LEC receives a packet to send and has neither a connection nor an ATM address, it requests the LES (on the Control Direct connection) for the ATM address associated with the destination MAC address. If the LES has the information, it will send the information to the LEC. If the LES cannot answer the request, it broadcasts the request to the LECs on this ELAN using the Control Distribute connection.

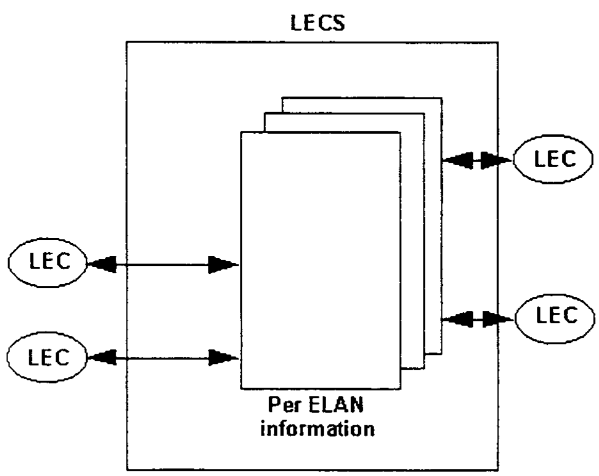


Figure 10.10: LECS (LAN Emulation Configuration Server)

The LECS maintains the database of configuration information for each ELAN, and there is one logical LECS per LAN Emulation Service. Typically, the network administrator initializes the database in the LECS.

LANE has the following disadvantages:

- It cannot resolve translational problems between technologies like Ethernet, token ring, and FDDI.
- A standard protocol for concurrent LEC registration to multiple LESs in the same ELAN does not exist.
- It does not support QoS capabilities that are inherent in ATM.
- It is only specified for UBR traffic. The support of the more efficient ABR traffic is still missing.

The ATM Forum LANE.v2 specification is currently being developed to overcome the disadvantages of LANE.v1. Although the IP (IPv4) protocols are the dominant forces in today's data communications, they also suffer from a number of problems. The new IP protocols, called IPng (IP next generation), offers the following improvements to the current IPv4 protocols.

- Header simplification and improved option support;
- Expanded routing and addressing capabilities;
- Security and authentication mechanism;
- QoS support;
- Transition mechanisms.

The IPng protocols are described in RFC 1752.

10.1.4 Multiprotocol over ATM (MPOA)

Classical IP over ATM or LANE are not the only means to support IP applications over ATM. The ATM Forum is working on another approach called Multiprotocol over ATM (MPOA). This new protocol should carry multiple protocols such as IP, IPX/SPX, and Appletalk over ATM, bypassing the routers. MPOA is a way to support layer 3 applications in an end-to-end connection with QoS features that LANE, operating at layer 2, does not support. The definition of MPOA includes NHRP (Next-Hop Routing Protocol) and MARS (Multicast Address Resolution Server). MPOA uses LANE and Classical IP over ATM. MPOA does three things:

1) It defines a high performance, low-latency way to support IP and other protocols over ATM.
2) It allows the network manager to build virtual subnets.
3) It permits applications to use the QoS features of ATM.

How does MPOA work? The following are the basic components of the MPOA model:

- ❒ Edge Devices;
- ❒ ATM-attached Hosts;
- ❒ Route Server;
- ❒ Internet Address Summarization Groups (ISAGs) or virtual subnets.

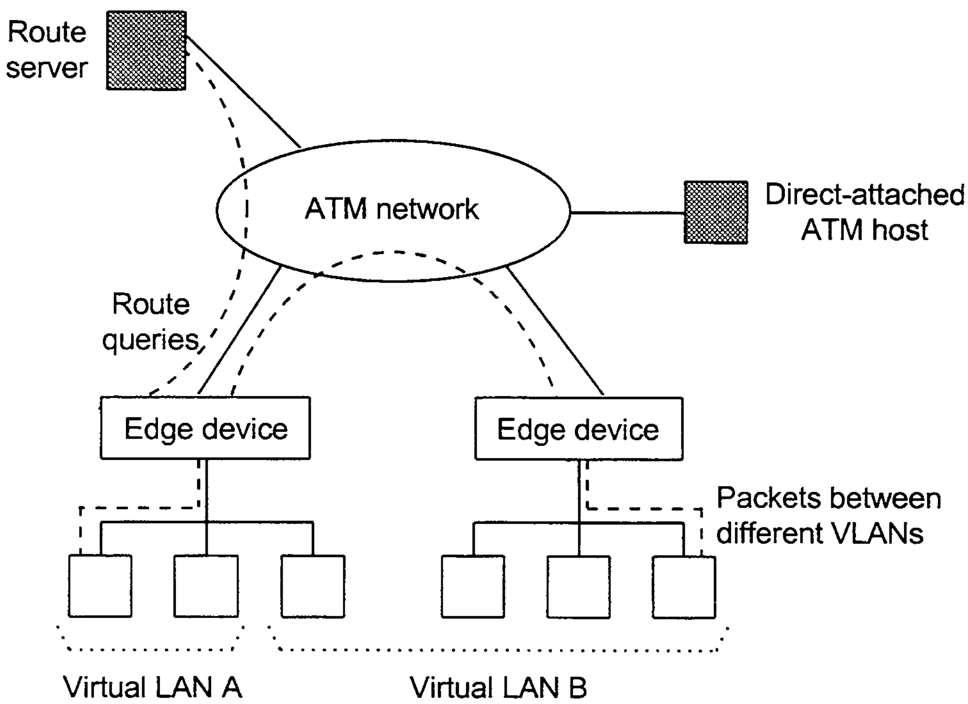


Figure 10.11: MPOA Model

Edge devices are intelligent switches. They use the network-layer or MAC-layer address of the destination to forward packets between legacy LAN segments and ATM interfaces. ATM-attached hosts are ATM adapter cards that implement the MPOA protocol. These hosts can communicate in an efficient way with each other or with the legacy LANs connected by an edge device. A route server maps network-layer subnets onto ATM, and can be implemented as a standalone entity or added to other existing routers or switches. One of the key benefits of MPOA is the ability to interact with virtual subnets, e.g., virtual LANs (VLANs). VLANs have become more common and gained importance in the last few years because configuring them is easy (logical topology is different from physical topology). In the current concept of an IP-Internetworking, one end system can reach other end systems in the same network directly. The end systems in other networks can be reached through routers, which have the following tasks:

- IP Routing and
- IP Forwarding.

Routers forward traffic to other networks using various routing algorithms such as OSPF and RIP; however, these approaches do not work in Non Broadcast Multiple Access (NBMA) networks like ATM or X.25. If the network is divided into smaller pieces, traffic will need to traverse additional routers and the end-to-end delay experienced by traffic will increase. NHRP is designed to overcome these difficulties, and uses the LLC/SNAP encapsulation like RFC 1483.

With direct connections over the network boundaries, the routers are less stressed and the number of hops is reduced. Route servers or route reflectors are used to reduce the routing problems. Two approaches exist to route traffic between the ATM layer and the Internetworking layer:

- Integrated Routing Model and
- Layered Routing Model.

Routing with the Integrated Model relies on a common database, and is integrated in the ATM and Internetworking layers. The Layered Model uses independent routing between the two layers.

Two models for addressing exists:

- Peer Addressing Model and
- Separated Addressing Model.

In the Peer Addressing Model, the Internetworking address of a system is unambiguous, whereas in the Separated Addressing Model, the Internetworking and the ATM addresses are different.

Multicast plays an increasing important role for supporting newer data applications. Classical IP over ATM (RFC 1483 or RFC 1577) supports only a unicast connection (point-to-point, bidirectional VCs). Multicasting can be implemented utilizing AAL5 with:

- Multicast Server or
- Direct Distribution.

With a Multicast Server, the transmitter sends packets to a central server, who distributes the packets using a point-to-multipoint connection to the receivers. With Direct Distribution, every transmitter sets up its own point-to-multipoint connection to each receiver and then sends the packets. LANE implements multicasting with the Broadcast and Unknown Server (BUS), which is a Multicast Server. The IETF is working on a new standard, the Multicast Address Resolution Server (MARS), which can use both the Multicast Server or Direct Distribution solutions. A proposed standard for MARS is RFC 2022 (Support for Multicast over UNI 3.0/3.1 based ATM Networks). RFC 2022 describes how ATM-based IP hosts and routers can support RFC 1112 style level 2 IP for a multicast transmission over the ATM Forum UNI 3.0/3.1 point-to-multipoint connection service. Its goals are as follows:

- Define a mechanism that allows UNI 3.0/3.1 based networks to support the multicast service of protocols such as IP;
- Define a mechanism to manage point-to-multipoint VCs to achieve multicasting for layer 3 packets.

In case of unicast IP, MARS uses the signaling technique described in RFC 1755 ("ATM Signaling Support for IP over ATM") to request for virtual channels with unspecified bit rate service.

10.2 Real-Time Applications

Older IP structures cannot be used to support real-time applications (voice, video, and real-time data), and other technologies such as circuit-switching networks have been developed for these applications. These technologies can be internetworked with ATM. This chapter describes how current technologies supporting real-time applications can run over ATM.

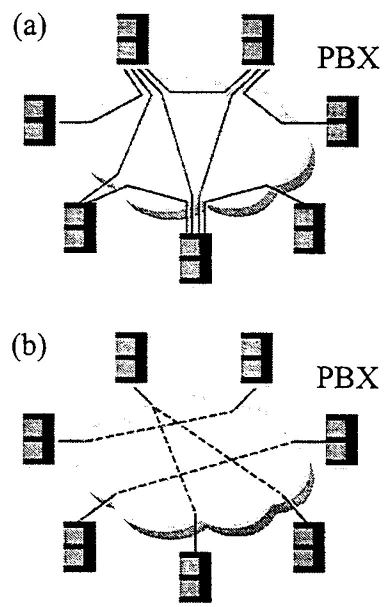
10.2.1 Circuit Emulation Service over ATM

The current LANs can be connected to ATM with LANE, which is defined for the most popular network types, Ethernet and token ring. The ATM Forum has also defined a similar service, referred to as Circuit Emulation Service (CES), for networks supporting real-time application. CES is classified into unstructured and structured types. The unstructured mode operates on a full 1.544/2.048 Mbit/s stream across a T1/E1 connection. It uses the AAL1 services, and requires no particular line framing and alignment between bytes and cells. The structured mode can support nx64 kbit/s streams across a T1/E1 interface with or without channel-associated signaling. Multiple framing, including extended super frame (ESF), is supported. The ATM Forum CES Specification I.363 describes how to support a Time Division Multiplexing (TDM) based network service over AAL1.

10.2.2 Voice over ATM

ATM must support voice, the dominant mode of human communication. There are two general strategies to achieve this goal. One is to overlay existing voice (circuit-switched) networks over ATM through CES, and the other is to develop native ATM voice applications to run directly over ATM.

Figure 10.12: PBX over ATM



One specification, which uses the the circuit emulation service (CES) of ATM, connects a PBX with a constant-bit-rate T1 or E1 interface to the ATM network (see Figure a). Permanent virtual circuits (PVCs) are used to emulate the voice channels in a simple but inefficient way. The original motivation of ATM is to exploit the bursty nature inherent in user applications like voice and data through statistical multiplexing. The ATM Forum VTOA (Voice and Telephony Over ATM) Working Group is trying to exploit the bursty or variable bit rate nature of voice.

Another solution to transmit voice over ATM, called voice trunking, has been defined by VTOA. Voice trunking (see Figure b) needs fewer channels and physical interfaces, since voice channels are supported through dynamic switched virtual connections (SVCs).

The technical details of VTOA have not been completed. In the interim, three approaches are used to integrate telephony with ATM.

In the first approach, the telephones are connected to the ATM network via a PhoneHub. All current PBX and inexpensive analog telephones can be used, and a desktop computer is not required.

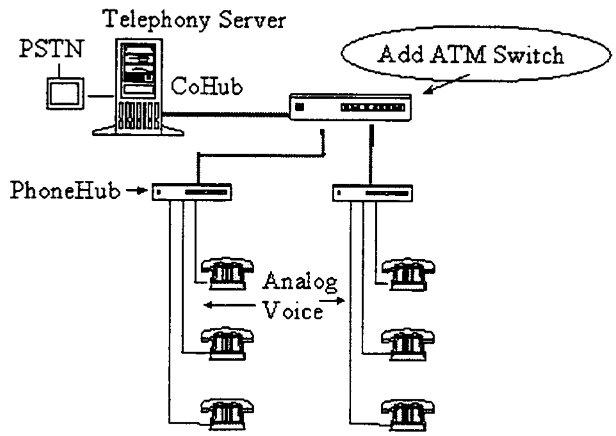


Figure 10.13: PhoneHub

In the second approach, the phone system is integrated into the existing LAN architecture. With this solution, called Computer Telephony Integration (CTI), the voice traffic is handled over ATM to analog phones as before, but now the PC takes over control and management functions of the phone system (e.g., call control, drag-and-drop transfer, handling of multiple calls).

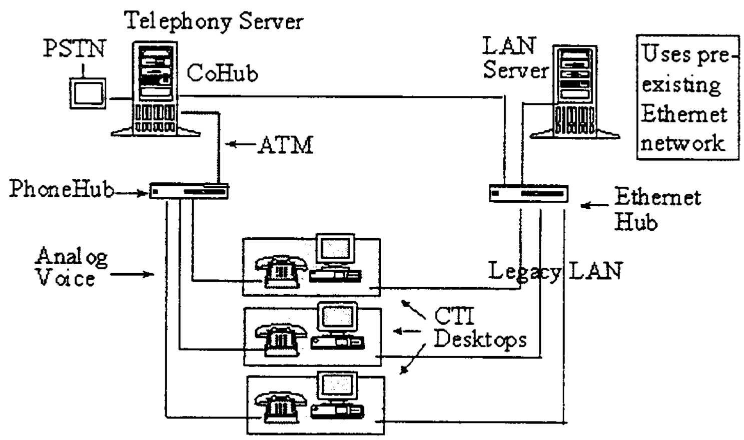


Figure 10.14: CTI

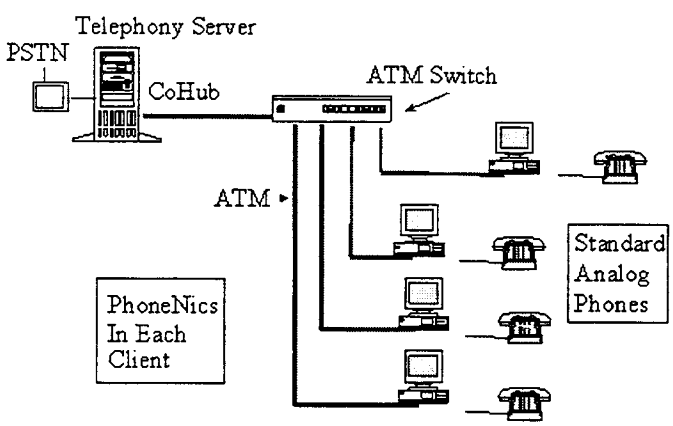


Figure 10.15: ATM PBX/LAN

The third approach is completely ATM-based. The PBX and LAN are connected via ATM connections up to the desktop. Special ATM Phone Network Interface Cards (NICs) permit signaling between an ATM switch and the computers, and voice traffic is encoded in ATM cells.

A hybrid of these three approaches can also be expected depending on the user requirements, costs, and the existing system.

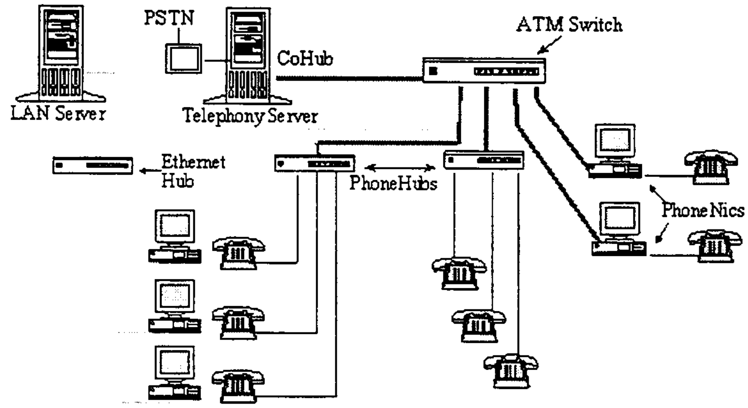


Figure 10.16: Mixed architecture

10.2.3 Video over ATM

Video transmissions usually need much more bandwidth than voice. The bit rate charcteristics of video applications differ depending on the coding and encoding schemes used. Video applications can be divided into three areas:

- Packetized video using the traditional LANs at the MAC or network layers;
- Constant-bit-rate video;
- Packetized video using codecs and an ATM adaptation layer.

Packetized video streams, usually IP-based, are designed to run over traditional LANs. They can also be transported over an ATM network through LANE, layer 3 encapsulation, or MPOA. A compression algorithm is often used to reduce the bandwidth required by these applications. Packetized videos often use a compression technique, e.g., MPEG (Moving Picture Experts Group) or JPEG (Joint Photographic Experts Group). Since video applications tend to have stringent delay requirement, it is preferable to transport them with certain QoS guarantees. Since traditional LAN architectures use best effort to transport traffic and provide no service guarantees, they need additional enhancements such as Protocol-Independant Multicast (PIM) or RSVP in order to support packetized video streams. Constant-bit-rate video runs over one or multiple ISDN-based 64-kbit/s lines and can be transported over ATM using circuit emulation. With a new specification from the ATM Forum, a more efficient utilization of bandwidth is possible through the use with MPEG2 compression and an AAL5 interface for RT-VBR traffic. The technical requirements for both real-time and non-real-time video are:

- Sufficient bandwidth;
- Low latency;
- Low jitter;
- Efficient multicast.

Many video compression and transmission standards supporting QoS exist:

- H.320: protocol for videoconferencing;
- H.221: protocol for convergence and multiplexing;

- H.261: protocol for video compression and decompression;
- MPEG1 and MPEG2: standard for video compression;
- MPEG4: standard for low-bandwidth videoconferencing;
- JPEG: standard for still picture (frame) compression;
- Motion JPEG: a standard to transmit moving pictures as a compressed JPEG image.

With a compression algorithm, the bandwidth can be reduced dramatically. The following table shows the compression ratios of various algorithms:

Standard/Format	Approximate Bandwidth	Compression Ratio
Motion JPEG	10-20 Mbit/s	7-27:1
MPEG-1	1.2-2.0 Mbit/s	1 100:1
H.261	64 kbit/s-2 Mbit/s	24:1
DVI	1.2-1.5 Mbit/s	160:1
CDI	1.2-1.5 Mbit/s	100:1
MPEG2	4-60 Mbit/s	30-100:1
CCIR 723	32-45 Mbit/s	3-5:1
CCIR 601/D-1	140-270 Mbit/s	reference
U.S. commercial systems using "mild compression"	45 Mbit/s	3-5:1
Vendor methods (e.g., Picture-Tel SG3)	0.1-1.5 Mbit/s	100:1
Software compression (small windows)	Approximately 2 Mbit/s	6:1

Figure 10.17: Bandwidth Requirement with Compression

How can an ATM network support real-time video applications? Depending on the bit rate characteristics of the applications, video can be transported over an ATM network in two ways as illustrated in Figure 10.18.

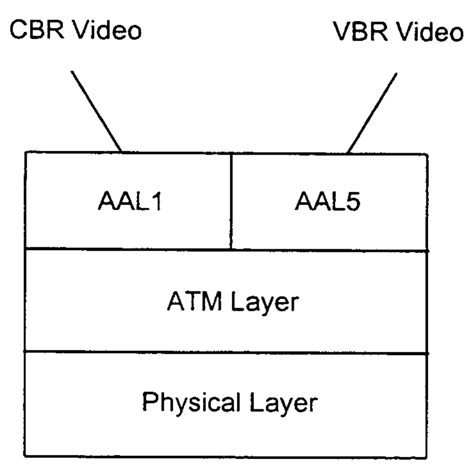


Figure 10.18: Video over ATM protocol stack

In a video application, an AAL1 interface with timestamp is used for CBR traffic and precise transmission clocking.

AAL5 supports bursty VBR or ABR video streams.

Application Type	LAN-based video	Distance video	Video on Demand (Cable TV/Telco TV)
Video Applications	Video courseware/ training Desktop videoconferencing Application sharing Graphic visualization Video kiosks	Remote classroom/ distance learning Videoconferencing Telecommuting Telemedicine Telejustice	Video on demand (VoD) Near video on demand (NVoD) Interactive video games
Video codecs and servers	PC-based codecs, hardware and software Video servers	Standalone codecs PC-based hardware and software codecs Video servers	Standalone codecs Set-top box Video servers
Video codec formats	MPEG, MPEG2, H.320 Proprietary motion JPEG	MPEG, MPEG2 MPEG4 (future) H.320/H261	MPEG2 Existing analog protocols (QAM RF modulation)
Network infrastructure: protocol and format perspective	Packetized video running over layer 2 or layer 3 Layer 2 or layer 3 internetworking with ATM	CBR video running over circuit emulation Packetized video over layer 2 or layer 3 Layer 2 or layer 3 internetworking with ATM	Packetized video running natively over ATM and Coax or ADSL Analog video using RF modulation
Network infrastructure: configuration	Highly segmented LANs with one or few users per segment ATM backbone ATM to desktop	Dedicated or on-demand WAN lines (leased lines, ISDN, etc.) Minimum 64 kbit/s for H.320 protocols Minimum 1.5 Mbit/s for MPEG protocols	ATM fiber networks to head-end and coaxial cable to home (hybid fiber coax) Fiber to the curb or home (FTTC, FTTH) ADSL
Network infrastructure: performance guarantees	ATM QoS ATM switched multicast circuits RSVP	ATM QoS ATM switched or permantent circuits RSVP	ATM QoS ATM switched or permantent virtual circuits
Network infrastructure: products	ATM switches LAN switches Routerswith LAN switching and ATM ports	Enterprise switches (support CBR, ATM and LAN connections)	Enterprise switches RF modulators for coaxial connections

Figure 10.19: Video applications

11 Wireless Connection to an ATM Network

While ATM was originally conceived to run on high-speed and low-bit-error-rate wire-based media, such as optical fiber channels, during the past several years, service providers are beginning to investigate the possibility of replacing or connecting the many existing mobile communication systems to a wire-based ATM infrastructure by a wireless network, which is commonly referred to as "'wireless ATM". Wireless ATM faces many additional challenges that are not present in the wireline ATM. The goal of this chapter is to provide a brief exposition on the issues currently being addressed by the wireless ATM community.

11.1 Wireless ATM Applications and Services

There are two general approaches for applications to utilize the transport infrastructure of a wireless ATM networks:

- ❒ Native mode ATM and
- ❒ TCP/IP over ATM.

In native mode ATM, which is also referred to as "Wireless ATM" (WATM), applications run directly on top of a wireless ATM network, with the support of an ATM adaptation layer (AAL).

Applications
AAL
Wireless ATM
Custom Wireless

Figure 11.1: Native mode ATM protocol stack for wireless ATM

In the TCP/IP over ATM mode, applications are transported by a wireless ATM network through the support of the TCP/IP protocol stack. This approach uses a "Wireless LAN" (WLAN) to make a connection to an ATM network. The original motivation behind WLAN is to connect an Ethernet network to mobile terminals using LAN Emulation (LANE).

Applications
TCP
IP
AAL
Wireless ATM
Custom Wireless

Figure 11.2: TCP/IP over ATM protocol stack for wireless ATM

It is conjectured that, as ATM technologies become mature, all applications will run directly on top of the wireless networks using native mode ATM. In the interim, however, it is expected that most data applications will utilize TCP/IP over ATM, due to the fact that most of today's data applications are IP-based. Non-data and new applications are expected to be transported through native-mode ATM. Regardless of the approach to be undertaken, the following issues must be addressed:

- What are the consequences when users are mobile, and move in and out of the range of a wireless connection?
- Which radio and frequency should be used?
- How much bandwidth is available?
- Where will the segmentation and reassembly be performed or where should the AAL be located?
- How is it possible to reduce the ATM overhead of about 10 percent (5 bytes header), which is too big for wireless networks?
- How is it possible to support the user's QoS requirements with high error rate links and mobile switches and users?

This chapter describes how these issues are currently being addressed by the wireless ATM community.

11.2 Technical Challenges not Present in Wired-Based ATM

11.2.1 Physical-layer Issues for Wireless ATM Networks

The key physical layer issues for wireless ATM networks are:

- How to determine the mode of radio operations in a bursty and multiaccess environment, and
- How to deal with moving terminals which resulted in multipath receptions at a base station.

While it is possible to resolve these issues through extra encapsulation, the overhead required may be too prohibitive for the wireless networks, in which bandwidth is already limited. For a wireless connection between a wireline ATM and an RF network, radio or infrared systems may be used depending on the following criteria:

- Frequency and bandwidth;
- Cost of the system;
- License;
- Indoor or outdoor environment;
- Number of users;
- Mobility (speed and distance between receiver and transmitter).

The switching technique is another consideration. ATM is form of packet-switching developed primarily for bursty or variable bit rate applications, but an RF network is typically designed for circuit-switched operations, in which a link is continuously active for data exchange, timing, and carrier recovery.

Which frequency should be used? The answer depends on the situation in which the wireless connection is used. The maximum practical operating frequency is about 10 GHz. The technology for an operation beyond 10 GHz does not exist today or is too expensive. Most systems will use high frequencies only if it is absolutely required. High attenuation is another problem in frequency ranges above 10 GHz. In the lower frequency bands, usage is heavily regulated by governments. In the U.S., the Federal Communications Commission (FCC) allocates the bands for various applications; in Europe, the European Telecommunications Standards Institute (ETSI) serves the analogous function of the FCC. Also, differences in allocation of bands among governments make networks inoperable across different nations.

Modern wireless systems for voice communication, e.g., the cell phones, often use the spread spectrum technique which permits a more efficient use of bandwidth. For data applications, the increase in efficiency is of secondary consideration. There are two types of spread spectrum techniques:

- Direct sequence and
- Frequency hopping.

Spread spectrum is only suitable for low bit rate applications and its cost of use increases dramatically in the high bit rate domain. While carrier and timing recovery is necessary in an RF network, it adds delay to the processing system. Special modulation techniques can reduce the delay but results in higher protocol overheads with the corresponding loss in efficiency. The main issue is to find a channel coding scheme to reduce the bursty wireless channel errors. There is no consensus in the literature as to what to use for error control on a wireless link; however, it is expected that the best solution would include channel error detecting and correcting codes, as well as cell-level forward error correction.

11.2.2 Data Link Layer Issues for Wireless Packet (ATM) Networks

The technique for transporting one protocol data unit (PDU) of one protocol into another is called encapsulation. The advantage of encapulation is protocol transparency; the disadvantages are added overhead and delay, which can be reduced by using cut-through techniques and header compression. In comparison to a fiber-based ATM network, the bit error rate in a wireless network is high, and techniques are required for detecting and correcting errors. The most common solutions are the automatic repeat request (ARQ) and the forward error correction (FEC) techniques. The most efficient solution is a combination of ARQ and FEC.

11.2.3 Media Access Layer Issues for Wireless Packet (ATM) Networks

Issues not present in a wire-based network are:

- Shared use of the broadcast transmission links and
- Mobility of users.

A media access control (MAC) allocates the use of a broadcast communication channel among multiple users.

The proper choice of a MAC protocol depends on the environment, and all protocols can be categorized into one of five groups:

- Fixed assignment;
- Random access;
- Centrally controlled demand assignment;
- Demand assignment with distributed contol;
- Adaptive strategies and mixed modes.

Fixed assignment techniques are used with stream-type traffic to support a high utilization of the communication channels and low response times, but this channel-oriented technique is inefficient for bursty traffic applications. A more efficient proposal for bursty traffic is a random access protocol, e.g., ALOHA or CSMA. These packet-oriented techniques allow one to use the full channel capacity for a short period of time on a random basis. The transmission capacity is allocated on a per-packet basis. With a demand assignment technique, the channel capacity is allocated to the user on a demand basis. It consists of two stages: a reservation stage followed by a transmission stage. A demand assignment protocol allocates a subchannel to a user if it requests bandwidth reservation. The reservation of the subchannel is usually based on a multiple access channel, e.g., TDMA or slotted ALOHA. In a centrally controlled system, the availability of a transmission depends on the reliability of the controller. This problem can be alleviated by using a distributed control technique. Adaptive strategies and mixed modes are used for different combinations of traffic types or time-varying mixtures. Every protocol has its advantages and limits, and the circumstances determine what to use. Most of the time, a channel is divided into several sections, each with its own protocols to support different conditions and traffic types.

11.2.4 Mobility Management

In a mobile environment, the users or the terminals move around; indeed, mobility is a key advantage of using a wireless network. The major problem is to track the mobile users. A database system is used to support the network in the tracking process. We assume that a network is geographically partitioned into subsystems or "zones" (Fig. 11.3). Every zone has radio port controllers, radio ports, and a database. The zones are connected to the wire-based ATM network infrastructure. The mobile users (symbolized by mobile phones and a vehicle in Fig. 11.3) move around. If the mobile phones only move around inside the zone, the link switches from one radio port to another and may be from one radio port controller to another. The database contains all information about the former conditions, the modifications, and the mobility of the users in the zone. The database is partitioned into two segments:

- A home segment for users permanently registered in that zone and
- A visitor segment for users that are visiting the zone.

The user with the mobile phones in Figure 11.3 will be registered in the home segment, whereas the vehicle entering the zone will be registered as a visitor. Every user has an identification number which allows the network to uniquely determine its location.

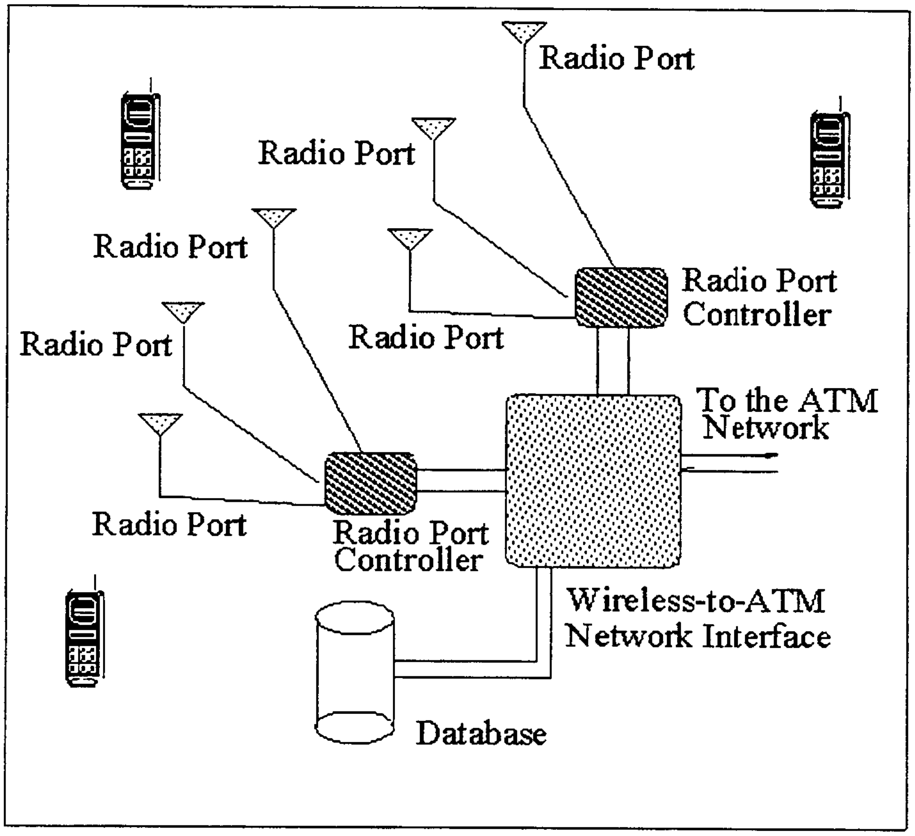


Figure 11.3: A typical zone configuration

To handle the mobility, it is necessary to have a scheme that would address the following issues:

- Location Management;
- Connection Management;
- Handoff Management.

The functions of the Location Management include tracking the position of a mobile (with its registration) and handling queries regarding the location of a mobile. For these tasks, two databases, home location register (HLR) and visitor location register (VLR), are required. Connection Management is necessary because the end points of a connection are mobile. It is important to maintain cell sequence and QoS in a wireless network to support a user's requirement. A handoff refers to the situation that one user moves and changes the link from one radio port to another radio port. The Handoff Management minimizes handoff time and packet loss during a handoff and allows a user to be truly mobile. The handoff, sometimes also called handover procedure, can be hard or soft depending on the user's mobility, which can be

- Intra zone,
- Inter zone or
- Inter network.

The more mobile a user, the more complicated is the management. If the mobile (symbolized as a vehicle in Fig. 11.3) enters the zone, it is necessary that the database of this zone gets all information about this user. The same data base information exchange is necessary if the mobile (symbolized as phone) leaves the zone. The information about the user's mobility and the exchange of such information between the zones and their databases usually take place at a backbone ATM network (Fig. 11.4). It is not recommended to use a link with a small bandwidth (e.g., an RF link) because the time for the information exchange will take too long and the data loss or delay is too big.

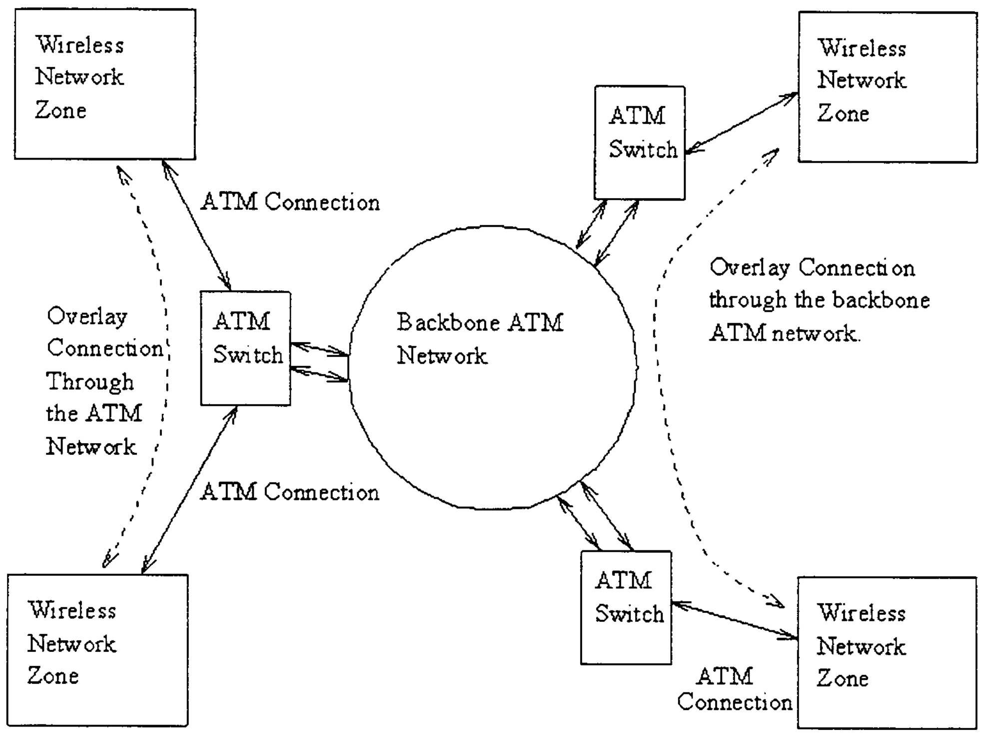


Figure 11.4: Overlay Signaling in the WATM Network

Only the mobility management for the case of mobile users has been explained. Although it is also possible to have mobile ATM switches, the management for handling the mobility is even more complicated. A solution for mobile switches has yet to be found or defined. All research projects described in the following chapter only address the case of mobile user. The ATM Forum and the ITU-T are examining the more complicate case of mobile switches. The requirements for seamless handover in wireless ATM networks have been identified as follows:

- Low latency;
- Scalability;
- QoS guarantee;
- Low signaling traffic;
- Minimal buffering;
- Data integrity;
- Group handover.

Solutions for user mobility management are being developed at this time.

11.3 Trends and Recent Advances

11.3.1 General Discussion

The support of a wireless connection to an ATM network is the subject of many active research studies. So far no general solutions have been developed, and each solution found would work only under a very specific environment. The IETF Mobile-IP working group has proposed a wireless ATM protocol architecture for a mobile terminal, a base station, and a switch (Fig. 11.5).

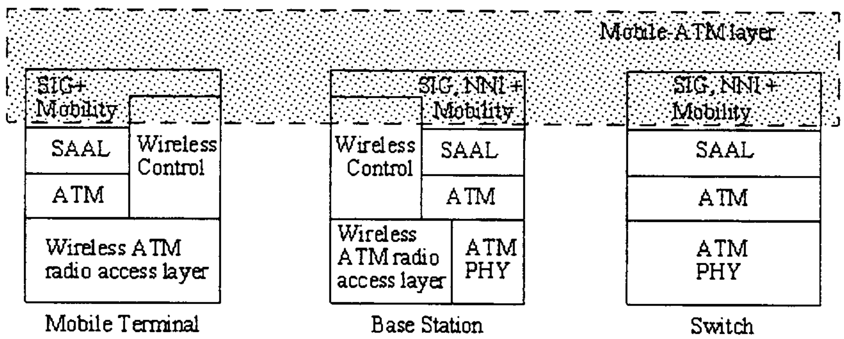


Figure 11.5: Proposed WATM Protocol Architecture

The proposal contains only a general architecture. The wireless ATM radio access layer is usually divided into:

- ❒ Wireless LLC-layer,
- ❒ Wireless MAC-layer and
- ❒ Wireless Physical-layer.

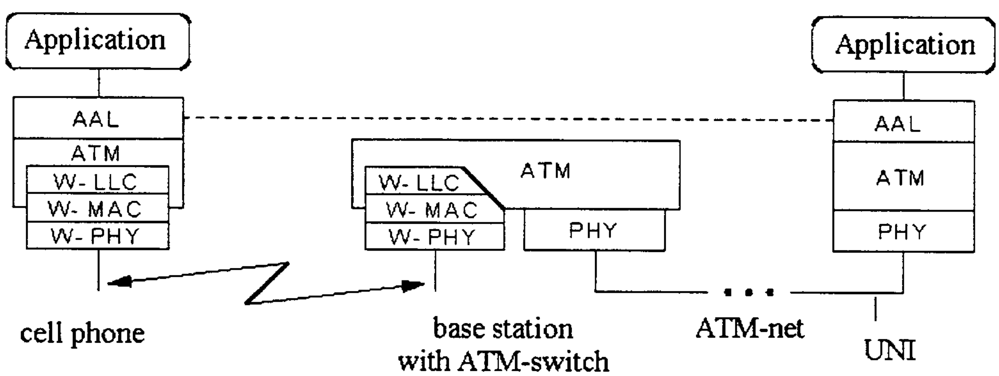


Figure 11.6: Protocol architecture of an ATM-RF-Interface

The following section gives a brief overview of the major current wireless ATM projects world-wide.

11.3.2 Seamless Wireless ATM Network (SWAN)

SWAN is a project developed by the Lucent Technologies, Bell Laboratories. Its goal is to test and develop an indoor wireless ATM network with room-sized pico-cells. The network operates around 2.4 GHz and supports data rate of up to 312 kbit/s. The mobility managment is mobile-initiated, and the decision of whether to handoff is based on measured station signal power.

11.3.3 Broadband Adaptive Homing ATM Architecture (BAHAMA)

The goal of BAHAMA, a project developed also by the Lucent Technologies, Bell Laboratories, is to design and evaluate a wireless ad-hoc ATM LAN/PBX concept, in which Portable Base Stations (PBSs) are the major components providing microcell coverage in an arbitrary topology. The concept offers the advantage of easy configuration, but there are drawbacks:

- Slow mobility (walking speed);
- Distributed intelligence for call routing and mobility management;
- Permission for mobiles to move through blind spots.

With a combination of FEC and ARQ, BAHAMA uses an efficient demand-assignment channel access protocol called Distributed-Queuing Request Update Multiple Access (DQRUMA). Mobility management is mobile initiated; that is, a mobile would initiate a handoff message when it recognizes a new PBS. The handoff message includes:

- The incoming and outgoing VCIs for the connections being handed over;
- The sequence number of the last received ATM cell;
- The identity of the previous Local PBS.

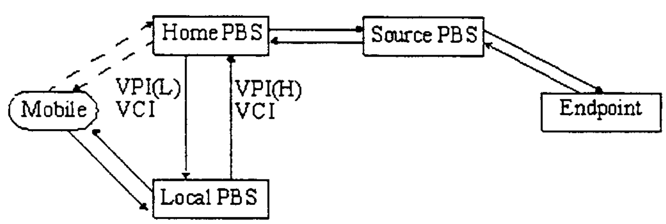


Figure 11.7: Channels in a handover procedure

In a handover procedure (Figure 11.7), the previous Local PBS is also the Home PBS for a mobile. The new Local PBS sends the old Local PBS the first three parameters with reverse channel identifier VPI(L)/VCI for the new segment from the Home PBS to the Local PBS. This message is sent through an out-of-band signaling channel as part of the Handoff-segment and Assign-channels message (Figure 11.8). After receiving these messages, the Home PBS deletes the mapping for the connection to the mobile and starts buffering the received cells from the Source PBS. Then it sends parameters in the Assign-channels message to the new Local PBS to inform about the received source-cells. After receiving this message, the new Local PBS selects VPI(H)/VCIs for the air interface, sets all mapping entries, and generates a Handoff-complete message to the mobile.

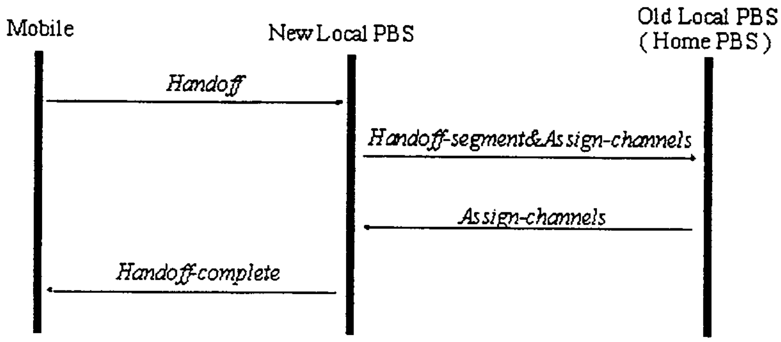


Figure 11.8: Handover messages

11.3.4 Magic Wireless ATM Network Demonstrator (WAND)

Magic WAND is supported by the European Advanced Communications Technologies and Services (ACTS). Its aim is to provide customers access to a wireless network. The project focuses on the mobility issues within an indoor domain. Typical applications which may benefit by the findings of Magic WAND are:

- An infrastructure replacement for a wired ATM access network in case of temporary office installations or installations into spaces where extensive cabling is not allowed. QoS provided must be close to that provided by a fixed network;
- Movable terminals used by nomadic workers. The QoS can be somewhat lower than the QoS of a fixed network;
- Application dedicated mobile systems, such as inventory control or surveillance, capable of operating at lower QoS.

The first proposal was to operate the system on a 17 GHz link, but the necessary equipment was not available. Now WAND is being developed in a 5 GHz band. The supported bandwidth is about 20 Mbit/s. A specific signaling protocol, a radio specific physical layer, and a MAC layer are used. For signaling, three different kinds of protocols have been proposed. The mobility management supports a forward and backward handover but a preference is given to the backward handover. The handover has the following features:

- All terminal connections are handed over at the same time;
- Part of connections can be released due to lack of resources;
- Uplink and downlink are switched together;
- Mobile does not oscillate between new and old access points;
- Hard handover will be used;
- Handover is started on demand by mobiles.

The connection specific processing in WAND is very close to standard ATM call processing.

11.3.5 MEDIAN

In the project MEDIAN (Wireless Professional and Residential Multimedia Applications), the ACTS develops a high speed wireless customer premises LAN as a pilot system for multimedia applications. The system uses the 60 GHz band, and is connected via an ATM interface to the 3rd and newer generations of mobile systems.

The main objectives are:

- To show the market that the future exploitation of very high speed 60 GHz WLANs is possible;
- Technological and commercial study of future 60 GHz MMIC components not only for use in MEDIAN;
- Technological and commercial study and implementation of VLSI solutions for very high data rate wireless systems;
- Development and future standardization of a high speed wireless customer premises local area network for multimedia applications in the 60 GHz range (with a net data rate up to 150 Mbit/s) connected to the fixed ATM network;
- To implement a pilot system, which consists of a base station and two portable stations providing a 150 Mbit/s duplex transmission;
- To demonstrate the performance in real user trials.

A typical application of MEDIAN is in an office environment:

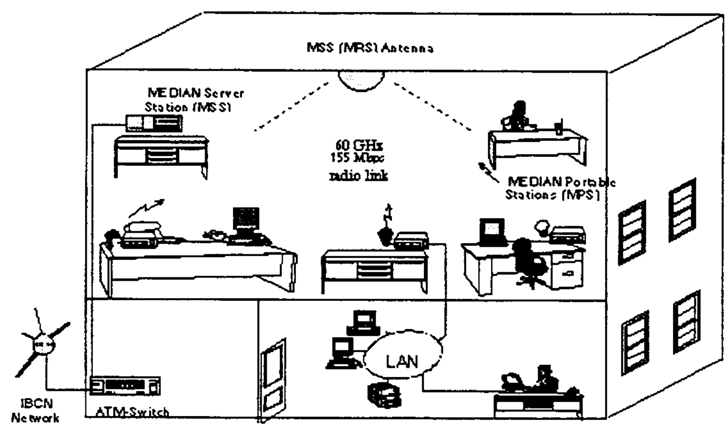


Figure 11.9: Typical MEDIAN Application Scenario

The ACTS also supports the projects SAMBA (System for Advanced Mobile Broadband Applications) and AWACS (ATM Wireless Access Communication System).

11.3.6 ORL Radio ATM

The Olivetti Research Limited (ORL) Radio ATM is an indoor wireless ATM system which operates in the 2.4 GHz range with a bandwidth of 10 MHz per channel for short range data links. The network is divided into pico-cells. Each pico-cell has a radius of approximately 30 feet.

Error control is accomplished by an ARQ which utilizes a 16-bit CRC and may retransmit a packet up to 10 times. The following entities are involved in the mobility control:

- Home Register (HR): records current proxy ATM address of a mobile, provides paging and notification services;
- Domain Location Server (DLS): registers a mobile within a domain, allocates the proxy address and FSP for the mobile;
- Mobile Switching Point (MSP): communicates with the current BSP and maintains tables of the link qualities and occupancy of neighbouring base stations;
- Base Switching Point (BSP): handles the management of the virtual path element between the base station and mobile;
- Fixed Switching Point (FSP): anchor-point for all virtual connections to the mobile;
- Base Manager (BM), Mobile Manager (MM): handle metasignaling between the mobile and the base.

The protocols for signaling in a wired ATM system defined by the ATM Forum UNI and NNI specifications do not support user mobility. The support of user mobility will be defined in a future ATM Forum specification. The project ORL Radio System solves the signaling problem in the case of user mobility by introducing another set of protocols which operate in parallel with the standard ones. The signaling mechanisms used are:

- Meta-signaling, which is used to establish signaling channels via an allocation of a VP to each mobile, in a situation where well-known permanent VCs cannot be used directly (e.g., broadcast channel to BS);
- Handover signaling, which performs the in-band switching of active VPs. Handover signaling for different mobiles uses separate VCIs;
- RPC (Remote Procedure Call) mechanism, which is used to provide machine independence for the location of management entities.

Prototypes of the system have been demonstrated in presentations to the public.

11.3.7 Mobile Broadband System

The European Commission of the Research and Development in Advanced Communication Services (RACE II) is investigating the Mobile Broadband System (MBS), a wireless ATM air interface between a B-ISDN network and mobile users. The overall goal of the MBS is to allow the integration of mobile ATM terminals with a fixed ATM network. More specifically, MBS focuses on the following issues:

- Development of channel access and logical link control protocols at the air interface, intelligent phase-array antennas, connection handling, handover control, dynamic channel management, mobility management, and security architecture;
- Formal specification of the protocols using the Specification and Description Language (SDL);
- Performance evaluation of the proposed protocols;

- Development of tools for radio coverage prediction; stochastic simulation of the protocols for performance evaluation for a given terminal mobility scenario description (e.g., indoors/outdoors) and mixture of traffic according to the service-specific cell streams of source terminals;
- SDL-based rapid prototyping of services and protocols to run WATM system demonstrators.

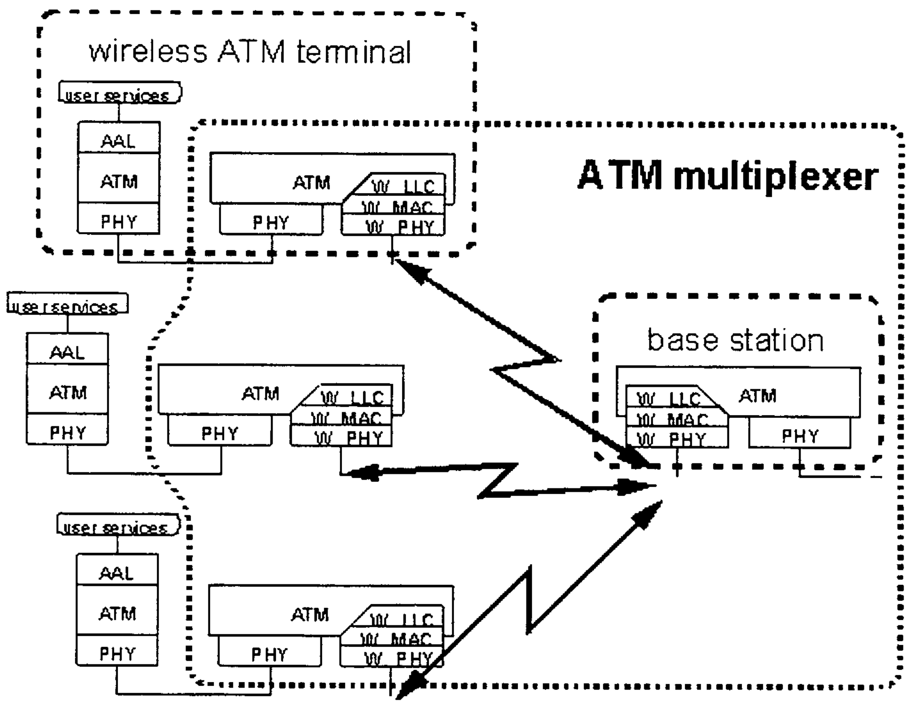


Figure 11.10: Architecture of an ATM air interface

M LLC: MBS Logical Link Control Layer

M MAC: MBS Medium Access Control Layer

M PHY: MBS Physical Layer

Since AAL is not involved in the integration of mobile ATM terminals, the radio link is integrated transparently into the ATM structure. Figure 11.10 shows the architecture in the lower protocol levels. MBS is designed for broadband transmission using frequency/time division multiple access (FDMA/TDMA) with maximum rate of up to 34 Mbit/s. The bandwidth can be increased by using four parallel modems with a total capacity of 155 Mbit/s. The system (indoor or outdoor) operates in a 60 GHz band in order to support these transmission rates. MBS can sustain video streams of 16 Mbit/s at 30 mph in the range of about 350 feet around a base station. The MAC protocol used is Dynamic Slot Assignment (DSA++). The DSA++ protocol functions are:

- Signaling of capacity (slot) assignments/reservations on the downlink by the base station controller;
- Transmission of capacity reservation request on the uplink (by inband signaling, random access, polling) by the mobile station;

- Service strategy in which the base station controller determines the order of ATM cell transmissions on the up- and down-links;
- Random access versus the polling mode of operation control (or both together);
- Fast collision resolution algorithm and stability control of random access protocol.

In comparison to a fiber link, the restricted transmission conditions on an air interface require an additional error correction scheme. This scheme is a hybrid combination of forward error correction (FEC) and automatic repeat request (ARQ), and is called Adaptive Selective Repeat Automatic Request (ASR-ARQ). MBS investigates the usage of adaptive directed antennas also. The advantages (higher gain, no or less inter-symbol interference, improved spectral efficiency) of these antennas create new problems, e.g., due to the difficulty in locating and tracking the mobiles, broadcast messages cannot be transmited with directed beams. Today a consensus solution on how to use special antennas does not exist.

11.3.8 ACTS ATM Internetwork (AAI)

The ACTS ATM Internetwork (AAI) in the U.S. is a research network to provide a wide area transport using the ATM technology. The project includes the connection of several DoD (Department of Defense) High Performance Computing centers (a subset known as the DREN Testbed), the MAGIC, and ATDnet gigabit testbeds.

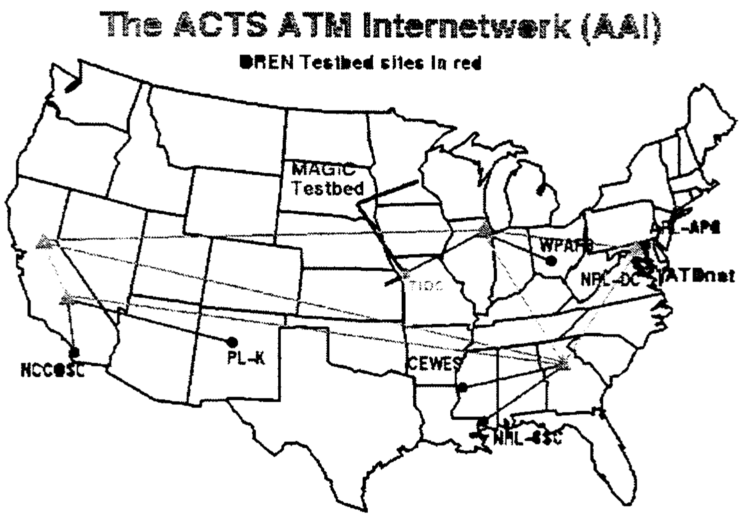


Figure 11.11: ACTS ATM Internetwork (AAI)

As the needs for wireless connection increase, the future AAI should support the wireless ATM technology. The goal of the Rapidly Deployable Radio Network (RDRN) project is to extend wireless ATM service to AAI. The work is done during a three year period at the Information and Telecommunication Technology Center (ITTC) of the University of Kansas under the sponsorship of the ARPA (Advanced Research Project Agency). The aim is to develop an ATM radio technology to support wireless ATM technology. The Rome Laboratories, a U.S. Air Force research center, together with the University of Kansas, is developing a wireless ATM Adaptive Voice/Data Network (AVDnet) to implement and demonstrate a complete adaptive voice/data network based on wireless ATM technology.

11.3.8.1 Rapidly Deployable Radio Network (RDRN)

The RDRN is an ATM-based wireless communication system. The prototype system consists of a Global Positioning System (GPS) receiver, a packet radio system for out-of-band signaling, and a wireless ATM interface. This system allows mobiles to integrate seamlessly into an end-to-end ATM based service infrastructure. The major components of the system are the Edge Nodes (EN) and the Remote Nodes (RN). The Edge Nodes consist of at least one Edge Switch (ES) and may contain an ATM switch. The Edge Switch has an OC-3 ATM port and a variable number of virtual ports that connect to the adaptive wireless network. It can generate multiple digitally formed beams, each with an independent modulation scheme. Depending on the modulation, one beam can have a data rate from 1 to 2 Mbit/s using a TDMA structure and can support up to 64 users.

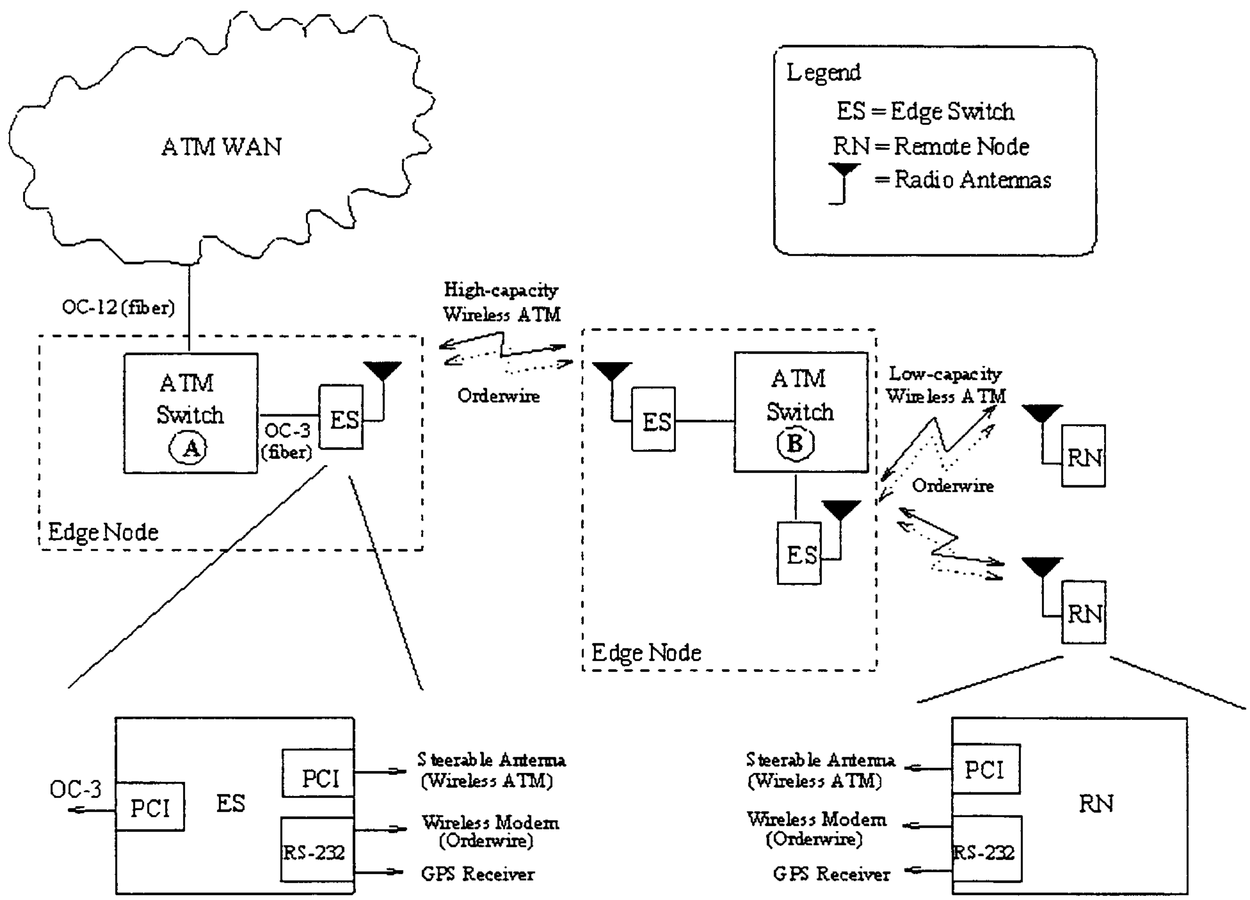


Figure 11.12: Typical Scenario

The system architecture has been designed to investigate the following key issues:

- Demonstration of a wireless ATM network and digital beamforming;
- Support research into adaptive software controlled radios;
- Demonstration of automatic network configuration/reconfiguration;
- Demonstrate interoperability with existing standardized ATM infrastructure.

With this system architecture, a mobile is allowed to move within a 6-mile range of an Edge Switch. The frequency used is the Amateur Radio Service (ARS) band, which ranges from 1240 to 1300 MHz. The minimum acceptable bit error rate without coding should be less than 10^{-5}. The following are the key features of the ATM/AAL level:

- Socket-based interface;
- Dynamic setup upon data protocol stack creation:
  - ATM address registration with local information server;
  - Well-known VC setup.
- EN/RN support:
  - CBR and UBR traffic types;
  - PVC and SVC connection types;
  - ATM ARP server (RFC1577);
  - Classical IP over ATM;
  - Mobile IP;
  - Raw and AAL5 (RFC1483) encapsulation;
  - Up to 1024 simultaneous reassemblies.

The investigation also includes the development of a specific antenna pattern. The antenna works directionally for an efficient spatial reuse. Two solutions for a handover procedure have been investigated:

- Tree based (Intermediate route changes);
- Home Agent based (Intermediate route must not change).

The features of the Tree Based Method include:

- Route from RN about to handoff forms a branch of a tree;
- Assign all possible VCIs to the RN (one for each ES to which it may handoff);
- A switch, which is the root of tree, will allow VC indirect index into the switch table based on which VCI and port RN a cell arrives;
- A switch will modify routes accordingly;
- No new call setup is required;
- All branch routes must remain in place indefinitely;
- ENs must have VCIs and wireless channels open for all possible RNs indefinitely to reduce the possibility of base station overload.

The characteristics of the Home Based Method are:

- Path between home switches never changes;
- Home switches may update slowly;
- Path lingers until cells are drained;
- Maintains cell order;
- Requires switching protocol modification.

11.3.8.2 Adaptive Voice/Data Network (AVDnet)

The aim of this project is to implement and demonstrate a complete adaptive voice/data network (AVDnet) for a narrowband link. The network should support dynamic bandwidth allocation between voice and data streams. The voice traffic is generated through a low bit rate speech coding based on the Sinusoidal Transform Coder (STC).

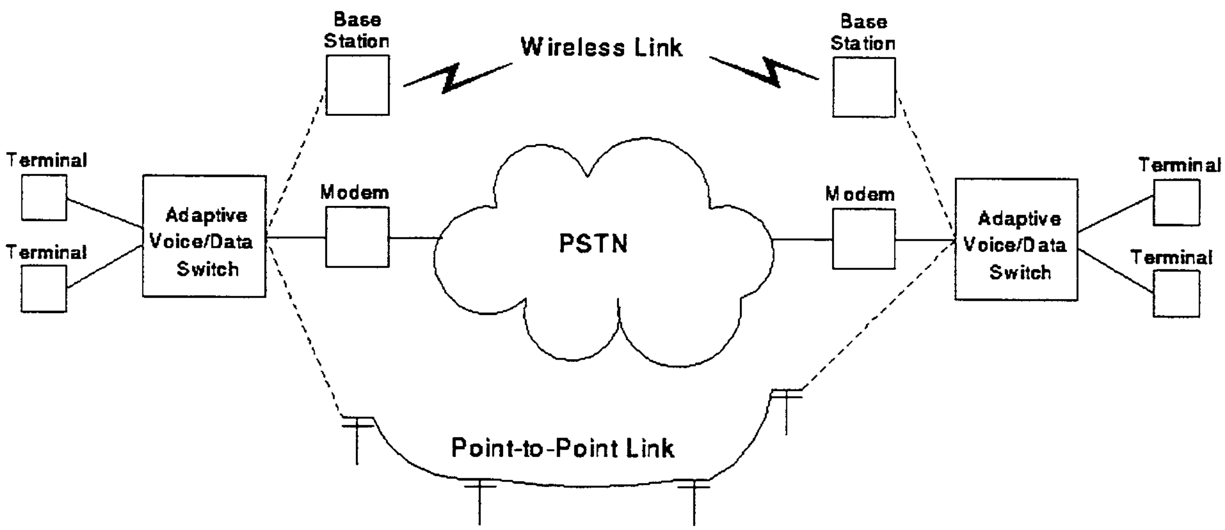


Figure 11.13: AVDnet environment

The major project tasks are:

- AVD switch modifications for ATM networks;
- Implementation of the terminal units for the AVD network;
- Development and implementation of the ATM wireless network architecture;
- Host application software design;
- Demonstration of interoperability over ISDN facilities;
- Demonstration of interoperability over future facilities typified by the DREN Testbed.

The narrowband network should be interoperable with other existing ATM facilities, e.g., the RDRN or the MAGIC gigabit testbed.

11.3.9 HIPERLAN (High Performance Radio LAN)

The ETSI Technical Committee RES10 (Radio Equipment and Systems) created a standard for a wireless LAN called HIPERLAN (High Performance Radio Local Area Network). It is a broadband radio system, and offers mainly local area network services. The aim is to support asynchronous service at rates of 1 to 20 Mbit/s and time bounded services at rates of 64 kbit/s up to 2048 kbit/s. The mobile HIPERLAN station is able to communicate while in motion at up to 20 mph. ETSI's aim is also to make HIPERLAN interoperable with IEEE 802.11, described in the next chapter. Here are some technical specifics about HIPERLAN:

Parameter	Traffic Type	Value
Data rate	asynchronous	1 to 20 Mbit/s
	time-bounded	64 kbit/s to 2.048 kbit/s
System throughput		20 Mbit/s to 1000 Mbit/s per hectare per floor
Mean latency	asynchronous	<1 ms. (at 30% capacity)
Latency of service initiation	time-bounded	<3 S
MSDU Delay variance	asynchronous	no limit
	time-bounded	<3.0 mSS
Range		to 50 m at 20 Mbit/s to 800 m at 1 Mbit/s
Area Coverage		99.9% (single hop)
Temporal Coverage		99.9% (single hop)
MPDU detected loss/error rate		<10-3
MPDU undetected loss/error rate		<8x10-8 per octet of MPDU length
MSDU undetected loss/error rate		<5x10-14 per octet of MPDU length
Co-location tolerance		50 cm of free space
Mobility tolerance		10 m/s linear, 360 degrees angular
Packet information field maximum size		16 kbytes
Physical size target (excl. antenna system)		PC-Card (PCMCIA) type III (85x54x10.5 mm)
Power consumption		few hundred mW

Figure 11.14: HIPERLAN features

Three different types of HIPERLAN exist. Type 1 and Type 2 operate at 5.2 GHz and are supposed to replace the wired LANs. HIPERLAN Type 2 is like a wireless ATM system. HIPERLAN Type 3 should operate at 17 GHz. The work is still going on. Currently, ETSI-RES10 is defining HIPERLAN Type 4 to improve the existing demonstrator in the following areas:

- Application of source/channel coding and intelligent antennas;
- Optimization of link layer protocols to match ATM bearer types;
- Feasibility of 40 GHz RF technology for ATM wireless LAN applications;
- Mobility management techniques together with the impact on the radio bearer appropriate for high bit rate communications.

The standard HIPERLAN Type 4 specification is used in the project AWACS (ATM Wireless Access Communication System).

11.4 Standards

11.4.1 Wireless LAN

The IEEE has decided to form a new global standard for the wireless LAN market. The protocol must handle fixed stations and portables, as well as mobile stations. The IEEE finalized a Wireless LAN standard called 802.11, which was ratified in July 1997. 802.11 defines a medium-independent MAC protocol sitting on top of a group of (medium-dependent) physical specifications.

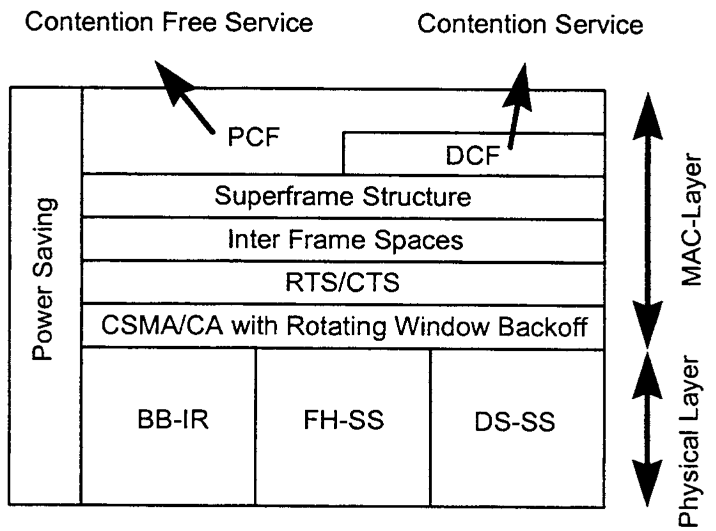


Figure 11.15: Elements of IEEE 802.11

The standard (802.11) defines three physical layers:

- ❒ Baseband Infrared (BB-IR),
- ❒ Direct Sequence Spread Spectrum (DS-SS) and
- ❒ Frequency Hopping Spread Spectrum (FH-SS).

The operation frequency range is at about 2.4 GHz. Data transfer of up to 2 Mbit/s is possible. The wireless coverage is about 50 to 200 feet. The selected MAC protocol in IEEE 802.11 is called Distributed Foundation Wireless MAC Protocol (DFWMAC), which provides two functions:

- A Point Coordination Function (PCF) for synchronous data transmission, and
- A Distributed Coordination Function (DCF) for asynchronous data.

DCF offers a contention service that is used for asynchronous traffic. PCF may also be used and offers contention free service for time bounded traffic or contention free asynchronous traffic. These two modes share the medium bandwidth in a time multiplexed manner. The access protocol to support the asynchronous communication between the stations is a CSMA/CA (Collision Avoidance) technique with the following features:

- Large differences in signal strengths;
- Collisions can occur only when:
    - Transmitter fails to get a response;
    - Receiver sees corrupted data through a CRC error.

The access mechanism can optionally be extended by RTS/CTS (Ready To Send/Clear To Send) message exchanges and is recommended if the payload of the packet exceeds a certain size.

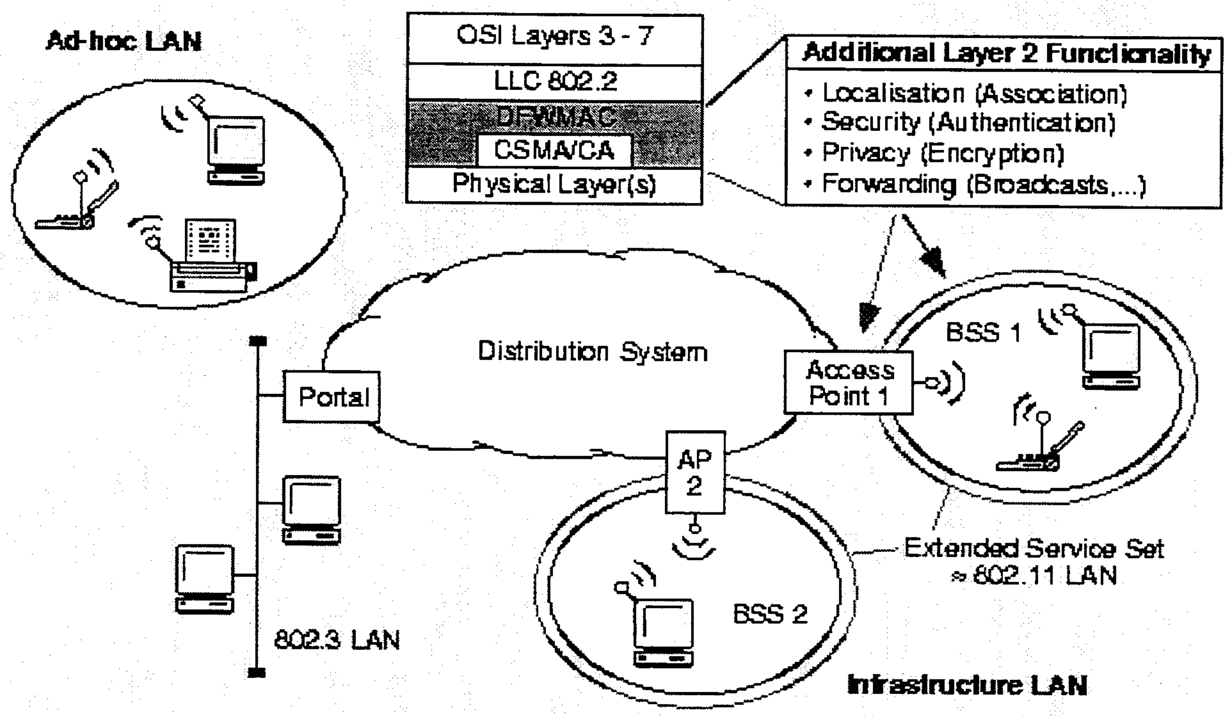


Figure 11.16: System architecture of 802.11

The IEEE 802.11 is a proposal for a common MAC layer standard for most LAN systems. This contrasts with the highly specialized system architecture proposed by the ETSI in its HIPER-LAN project.

11.4.2 Wireless ATM

The ATM Forum is working on several specifications for a wireless ATM network:

- Radio Access Layer and Media Access Control Requirements Definition;
- Mobility Management;
- Location Management;
- WATM Spec 1.0.

Version 1.0 of WATM is expected to be completed by 02/99, whereas the others should be finished by the summer of 1997.

11.4.2.1 Issues

Even though the specification is not completed, there are many ongoing discussions on a handover solution in a wireless ATM network in the ATM Forum Technical Committee.

The proposed requirements are:

- Handover latency;
- Scalability;
- Quality of Service;
- Signaling traffic;
- Buffer strategy;
- Data integrity;
- Group handover;
- Registration and authentication.

The issues for the handover are:

- Path extension versus path rerouting;
- Static versus dynamic crossover switch selection;
- Control plane versus user plane handover signaling;
- Backward and forward handover.

The requirements for the physical layer, the medium access control layer, and data link control layer of a wireless ATM system have been discussed and defined:

❒ Physical layer requirements:

- Frequency bands;
- Data rates;
- Error rates;
- Range and transmission power;
- Modulation efficiency;
- Channelization;
- Turnaround time.

❒ Medium access control layer requirements:

- Access point or ad-hoc;
- Quality of Service;
- Framing structure;
- Addressing;
- Power saving.

❒ Data link control layer requirements:

- FEC and ARQ techniques.

Many scenarios for wireless ATM have been discussed. The solutions of various projects include indoor system (or also called "In-Building") as well as outdoor systems. Last Hop is an expression for a wireless ATM provision from public ATM services to buildings.

The following table provides a detailed comparison of different scenarios:

	In-Building	Last Hop
Frequency Band	5 GHz HIPERLAN/NII/SUPERNet	60 GHz
Data Rate	25 Mb/s per cell	155 Mb/s per cell
Range	< 30 metres	< 300 metres
Number of Users (avg.)	< 10	< 50
Number of Users (max.)	< 100	< 100
Transmission Power	< 100 mW	< 100 mW
Target BER	10^{-4}	10^{-6}
Turnaround Time	< 5 μs	< 5 μs
Handover Support	Yes	No
Portability	Yes	No

Figure 11.17: In-Building and Last Hop specific requirements

Another unsolved problem is the location management of mobile ATM devices. In various projects, the problem has been investigated and different solutions have been developed. There is an on-going discussion by the ATM Forum Technical Committee about the use of tunnelled signaling technique in combination with a location service to manage user mobility. Tunnelling is a technique to describe the encapsulation of an endpoint address in a message routed via an intermediate address called the tunnel address. This scheme is applicable to the scenarios in which the wireless link is to a mobile terminal and one in which the link is to a mobile. The advantages of the tunnelling approach are:

- Compatibility with UNI/PNNI/B-ICI;
- No management load for intermediate switches;
- Routing efficient with mobile enabled networks;
- Network functional with no mobile enhancements;
- Reduces dynamic routing problem in local area;
- Can reduce binding overhead especially for mobile networks.

Disadvantages are:

- Address partition required between mobile and fixed addresses;
- Location service required.

The most important feature is that this scheme can operate without any changes to signaling protocols and, therefore, can work with existing and future systems.

11.4.2.2 Drafts and Proposals

The ATM Forum Wireless ATM Working Group is developing a set of specifications to facilitate the use of ATM technology for a broad range of wireless access network scenarios. These specifications should be a reference architecture for wireless ATM networks, private as well as public, and will consist of two major components:

- Radio access layer dealing with radio link protocols for wireless ATM access;
- Mobile ATM dealing with higher-layer control/signaling functions needed for generic mobility support.

A proposed specification has been defined and will be introduced in this chapter. Its aim is to create a future seamless wired and wireless multimedia network concept. This also includes the integration of various existing technical approaches for broadband wireless networking, high-speed packet-switched wireless LANs, wireless ATM, as well as "third-generation" circuit-oriented PCS/cellular. In addition, the concept should support mobility in the ATM networks, independent of the wireless access technology (e.g., GSM, IS-54 TDMA, IS-95 CDMA, PHS, IEEE 802.11, etc.) used. In the case where mobile communication services over an ATM infrastructure are required, the specification recommends the addition of "mobile ATM" functionalities to existing signaling/control protocols for supporting terminal mobility (Fig. 11.18).

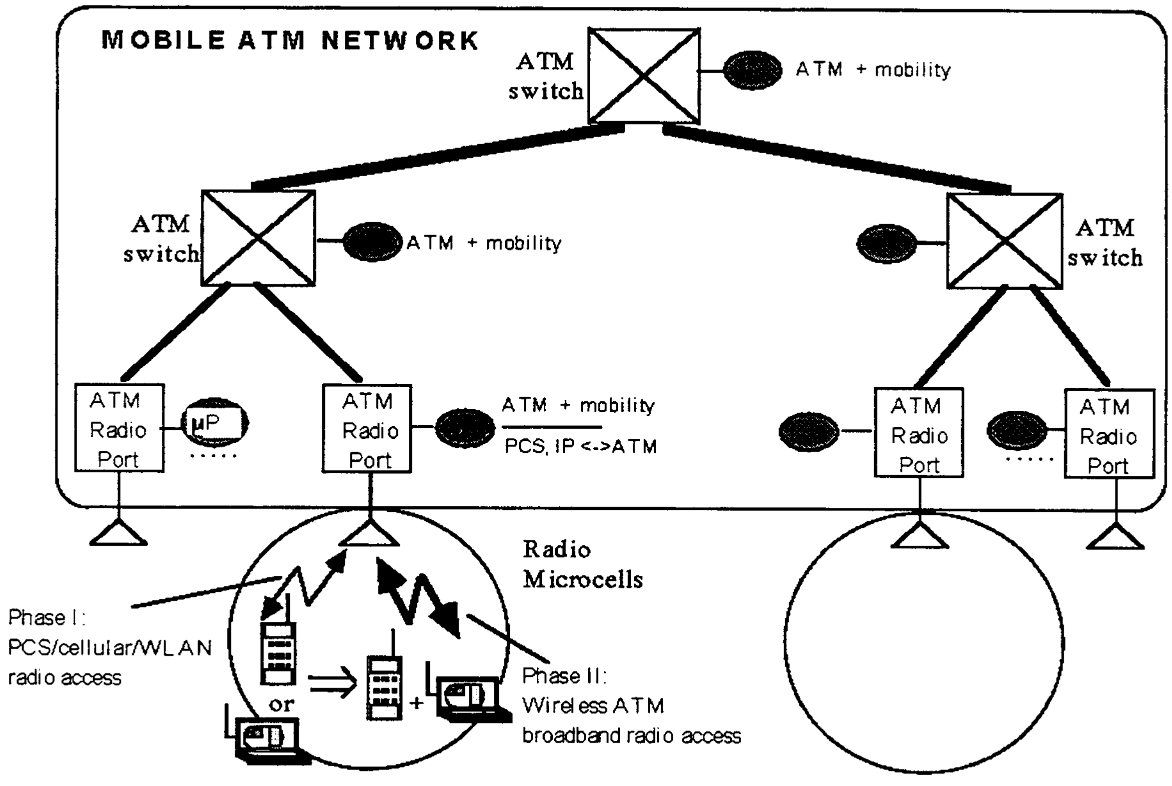


Figure 11.18: Mobile ATM network concept

11.4.2.3 Wireless ATM System Architecture

The basic idea of a wireless ATM proposal is to use the standard ATM cell for network level functions, while adding a wireless header/trailer on the radio link for wireless channel specific protocol sublayers (medium access control, data link control and wireless network control) as shown in Fig. 11.19.

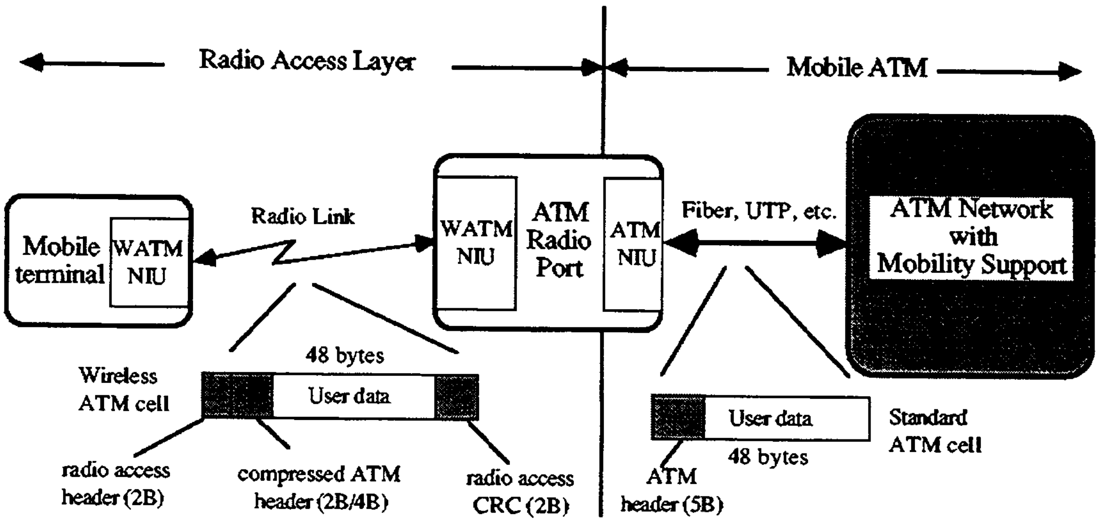


Figure 11.19: Wireless ATM network concept

The proposed wireless ATM protocol has to be fully harmonized with that of the standard ATM. The solution is to integrate new wireless channel specific sublayers (physical, medium access control, data link control, and network control) into the ATM prococol stack (Fig. 11.20). The advantage is that normal ATM network layer and control services, e.g., E.164 or IP-over ATM addressing, VC multiplexing, cell prioritization, congestion/QoS control, Q.2931 signaling for call establishment can be used for mobile services.

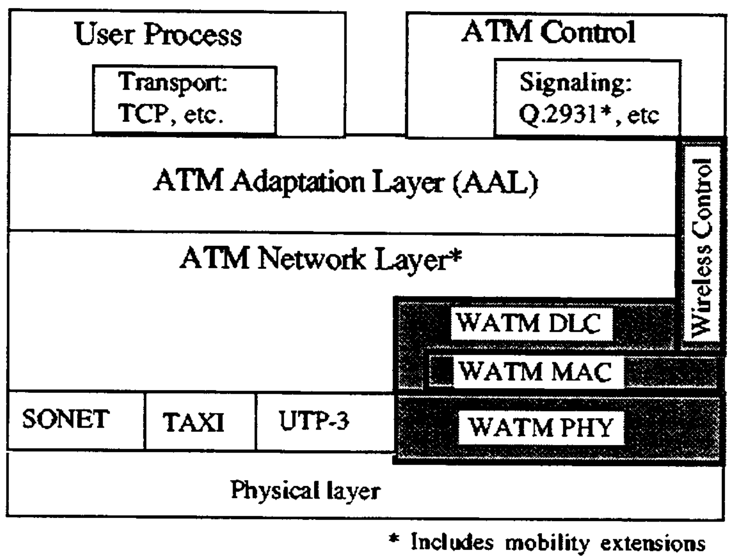


Figure 11.20: Wireless ATM protocol stack

As mentioned before, the wireless protocols, architecture, or cells should look like the standard ATM specifications. Figure 11.21 is an example of the format of wireless ATM cells and related wireless control packets used for data link control acknowledgments and radio link metasignaling.

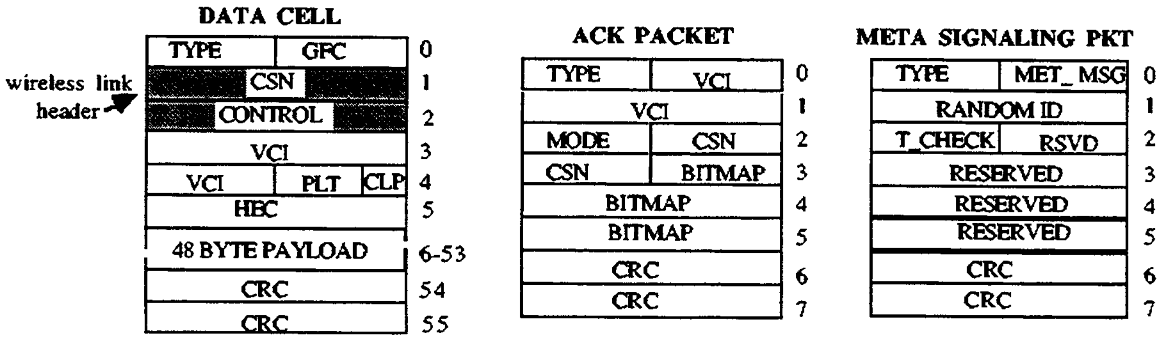


Figure 11.21: Typical wireless ATM cell and control packet formats

Based on the above design concepts, the ATM Forum Technical Committee created a formal reference architecture for wireless ATM for use in future specification activities (Fig. 11.22). The overall system specification consists of a radio access segment and a fixed network segment.

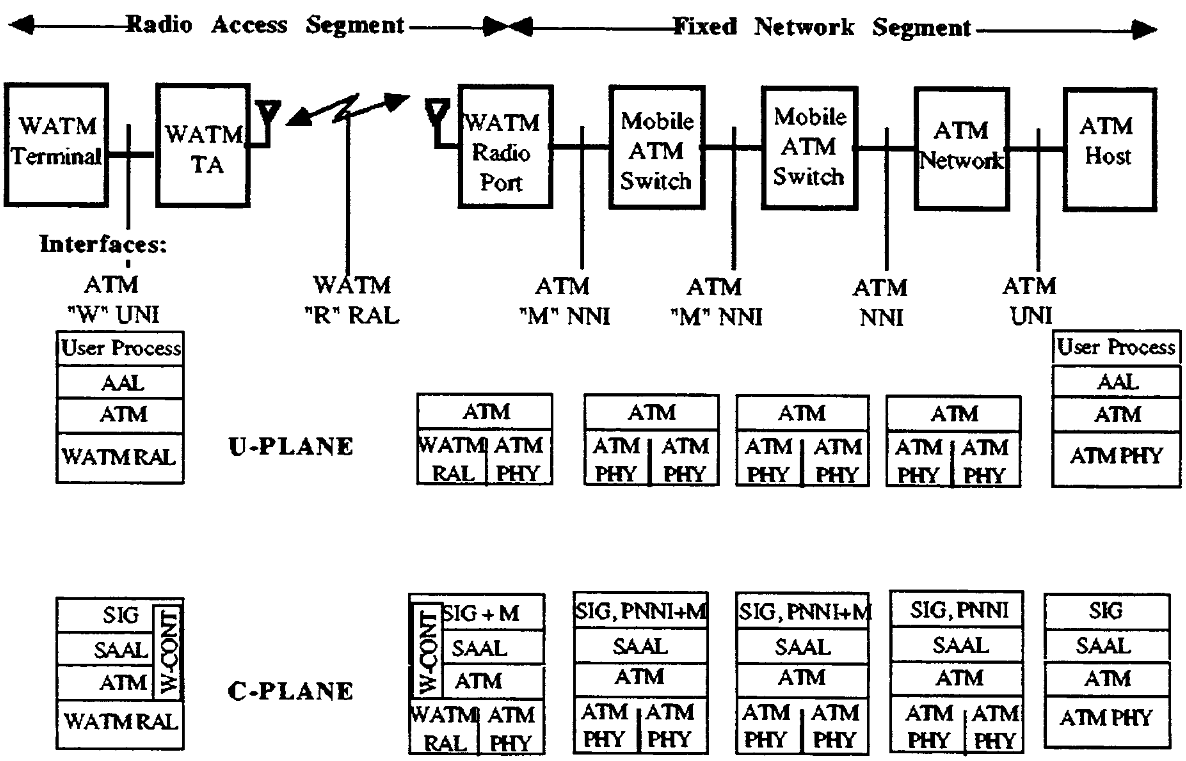


Figure 11.22: Wireless ATM System Reference Model

The fixed network segment may be defined in terms of several optional "M" (Mobile ATM) UNI/NNI specifications which incorporate mobility support extensions to the existing standard ATM UNI/NNI specifications. The wireless segment for end-to-end ATM (including radio MAC, DLC, and PHY) may separately be defined in terms of an optional "R" (Radio Access Layer, RAL) specification. The union of these optional "M" and "R" ATM specifications will define the complete wireless ATM "W" specification. The major components of the wireless ATM system reference model are:

- WATM Terminal: the end user device;
- WATM Terminal Adapter: the wireless ATM network interface at end-user;
- WATM Radio Port: the radio interface to the fixed ATM network;
- Mobile ATM switch: the access switch with mobility suport capabilities;
- ATM Network: the standard fixed ATM network;
- ATM Host: a standard ATM end user/server device.

11.4.2.4 Subsystem Design

A wireless ATM system consists of a radio access layer and a mobile ATM network with the following key design components:

- "Radio Access Layer" protocols:
  - High-speed radio physical layer (PHY);
  - Medium access control (MAC);
  - Data link control (DLC);
  - Wireless control.
- "Mobile ATM network" protocol extensions:
  - Handoff control;
  - Location management;
  - Routing and QoS control.

In the following, a brief outline of the technical scope for both components is given.

Radio Physical Layer:

- Microcell or picocell environment with radius in the range of 100 to 500 meters;
- Bit rates of about 25 Mbit/s or higher, with short burst preambles (e.g., 16 bytes max);
- Efficient frequency usage (2 bit/s per Hertz or higher);
- Power level 100 mW or lower;
- Low bit error rate ;
- Modulation methods: QPSK/QAM, multicarrier OFDM, spread spectrum CDMA.

Scope includes (but is not limited to):

- Microcellular arrangements (antennas, radio cell radius, power levels, frequency reuse, etc.);

- Basic modulation method, bit-rate, signal spectrum, etc.;
- Diversity, equalization, multicarrier adaptation, code selection, FEC, etc.;
- Radio channel data format, including burst preamble, training sequences, coding, security encryption, etc.;
- Data and control interface to radio modem (PHY).

Medium Access Control:

- Supports the use of the radio channel by multiple terminal devices;
- Supports required QoS levels and maintains a reasonably high radio channel efficiency;
- Techniques for the WATM MAC layer are PRMA extensions, dynamic TDMA/TDD, and CDMA.

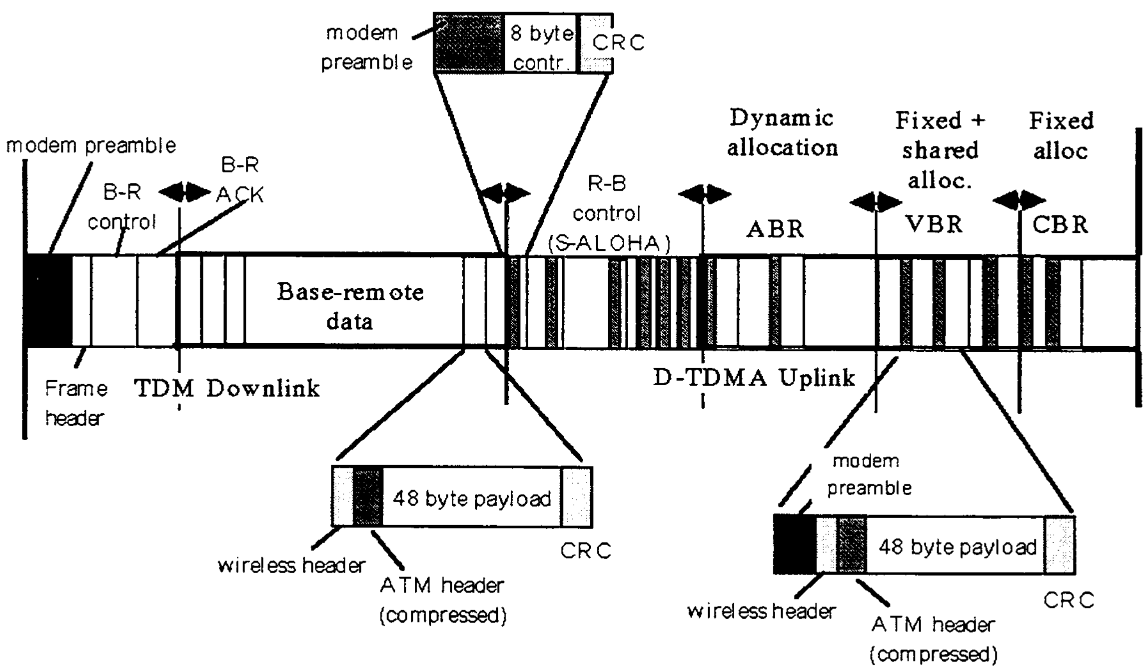


Figure 11.23: Dynamic TDMA/TDD protocol for wireless ATM access

One solution, the dynamic TDMA/TDD protocol (Fig. 11.23), allocates the ABR and VBR slots and periodic assignment of isochronous CBR slots frame-by-frame. Downlink (e.g., radio port or remote station) control and ATM data are multiplexed into a single TDM burst. Uplink control packets (including request for VC allocation) are sent in a slotted ALOHA contention mode in a designated region to the frame, while ATM user traffic is transmitted in slots allocated by the radio port controller. ABR slots are assigned dynamically on a frame-by-frame basis, while CBR slots are given fixed periodic slots assignments when a new (or handoff) call is established. VBR service may be provided with a suitable combination of these periodic and dynamic allocation modes.

Scope includes (but is not limited to):

- MAC protocol and syntax definition, including data format, framing, control, etc.;
- MAC control algorithms for each ATM service with QoS control, etc.;
- Interface to PHY layer, and special PHY requirements if any;
- Interface to DLC layer, and special support for link-layer protocols if any.

Data link control:

- DLC for ABR: traditional SREJ ARQ procedures on a burst-by-burst basis, without time limits for completion;
- DLC for VBR and CBR: use of a finite buffering interval that is specified by the application during VC set-up.

Scope includes (but is not limited to):

- DLC protocol and syntax, including wireless headers, control messages, FEC, etc.;
- DLC procedure options for ABR, VBR, CBR, and UBR;
- Interface to MAC layer, and special MAC requirements if any;
- Interface to ATM network layer.

Wireless control:

- Radio resource control and management functions at the PHY, MAC, and DLC layers;
- Terminal migration;
- Handoff control.

Scope includes (but is not limited to):

- Control/management syntax for PHY, MAC and DLC layers;
- Metasignaling support for mobile ATM;
- Interface to ATM control plane.

Handoff control:

- Dynamic support of terminal migration;
- Use of rerouting mechanisms.

Scope includes (but is not limited to):

- Signaling syntax for handoff, e.g., new Q.2931 signal for path change/extension;
- CAC/QoS control and renegotiation capability during handoff;
- Option for OAM cells to facilitate seamless handover;
- NNI features for periodic route optimization (e.g., loop removal);
- Public network aspects.

Location management:

- Uses mapping capability to locate the current endpoint to which the device is attached;
- Algorithms for a location management are based on methods used in other wireless communication systems.

Scope includes (but is not limited to):

- Network reference model for both integrated and external location management options;
- Interface with public PCS/cellular location management services (e.g., GSM MAP, IS-41, etc.);
- ATM addressing principles (E.164, ATM domains, etc.);
- Protocol syntax for mobility management (for address updates, queries, etc.);
- Mobile user authentication, registration, etc.

Routing and QoS control:

- Extensions to existing routing algorithms to deal with route changes and optimizations associated with handoff;
- Various approaches (e.g., re-optimizing the original route, straighforward path extension techniques);
- Mapping of mobile terminal routing-ID´s to paths in the network.

Scope includes (but is not limited to):

- Name-to-location resolution (implications for LANE, MPOA, etc.);
- Link-layer support to detect location changes & reconfigure parameters;
- NNI upgrades for handoff (path change, extension, loop removal, etc.);
- Routing-ID syntax, "invariant" call descriptor, etc.;
- Public network aspects;
- Additional syntax requirements for mobile CAC, if any;
- Extensions to ABR control policy during handoff, etc.;
- Support for dynamic QoS renegotiation to deal with change of resources after handoff.

11.5 Future Outlook

The Wireless Mobile ATM Task Force will host its 1st International Workshop on Wireless Mobile ATM (wmATM) Implementations on April 6 thru 10, 1998 in Hangzhou, China.

The following issues will be addressed at the Workshop:

- Medium Access Control protocol for wmATM;
- High-speed Coding/decoding for ATM cell transmission;
- Mobility configuration protocol for wmATM;

- Signaling protocol for wmATM;
- Effective forwarding protocol with Handoff for wmATM;
- Resource reservation protocol for the Wireless media;
- Mobile MIB for the wmATM management;
- Mobile X Window and Mobile Teleporting system;
- Multimedia transmission protocol over wmATM;
- QoS guarantee across the wmATM;
- Flow control protocol for wmATM;
- Congestion Avoidance protocol for wmATM;
- Effective Physical Layer Implementation for wmATM;
- Wireless AAL issues for wmATM;
- TCPng/IPng issues for wmATM;
- CDMA-ATM issues;
- DECT-ATM issues;
- WLL-ATM issues;
- ATM over Satellite issues;
- Millimeter Wave issues;
- Wireless Shared Media issues.

11.6 Feasibility of Wireless ATM

While wireless ATM faces many difficult issues, there is little doubt that it will exist in the future due to the explosive demand of wireless communication services. The large number of current wireless networks will require many interfaces. It is also necessary to adjust the system in different and varying conditions (range, bandwidth, number of user, mobility, wheather conditions, jamming) to support the QoS requirement of the users. Today, the industry and various standardization organizations are debating the issue of how to develop a wireless ATM network. The industry wants to develop the equipment for mobile users first and for mobile switches later, whereas the organizations want to create the standards for an all-including environment with mobile users as well as mobile switches. A complete solution is unlikely to be finalized by next year because of the technical difficulties cited. The following figure shows the possible relationship between the degree of user mobility and the corresponding data rate supported for a few wireless communication systems. Included in the figure are new wireless phone systems, the Global System for Mobile Communications (GSM), 2nd generation mobile phone systems, and the Universal Mobile Telecommunications System, a 3rd generation mobile system.

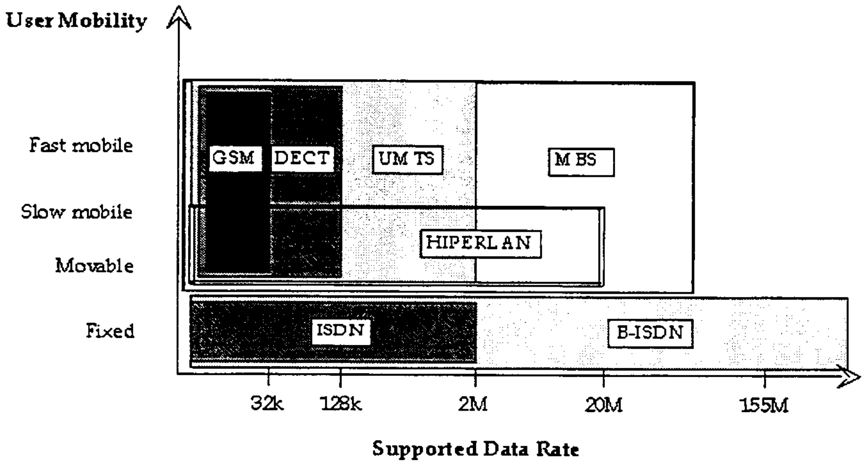


Figure 11.24: Supported Data Rate and User Mobility of various wireless systems

It is important to mention that most of the described projects are in a research phase. The solutions are being evaluated in the laboratories and have not been offered by vendors. In conclusion, I conjecture that Wireless ATM is feasible, but it is expected that the deployment of a wireless ATM system that can support both broadband communication services and high user mobility will require a significant amount of time and resources.

12 Security in ATM Networks

12.1 General Discussion

Security in networks has become more important as the need to protect the involved system, lines and the processed information against a threat from outside or inside increases. Networks are connected to each other and it is not possible to isolate a network from others. This is especially true for ATM networks which support the connection to most other network technologies with the current interfaces and protocols. This chapter describes the measures to make an ATM network secure. Customers (service subscribers and users), operators (network operators and service provider) and public communities/authorities have different requirements for a security in ATM networks. In the following, different objectives are listed as examples to explain the variety.

Customer objectives are:

- Availability and correct functionality of service subscription, activation, and deactivation;
- Availability and correct functionality of the ATM network services;
- Correct and verifiable billing;
- Data integrity/privacy and confidentiality;
- Capability to use a service anonymously.

Operator objectives are:

- Availability and correct functionality of the ATM network services;
- Availability and correct functionality of the ATM network management;
- Correct and verifiable billing, above all no possibility of fraud;
- Non-repudiation for all used ATM network services and for all management activities;
- Preservation of reputation (above all preservation of customers' and investors' trust);
- Accountability for all activities;
- Data integrity/privacy and confidentiality.

Public objectives are:

- Availability and correct functionality of the ATM network services;
- Data privacy and confidentiality.

Although user requirements for security are different, they share several common objectives:

- Confidentiality: Confidentiality of stored and transferred information;
- Data Integrity: Protection of stored and transferred information;
- Accountability: Accountability for all ATM network service invocations and for all ATM network management activities; any entity should be responsible for any actions initiated;
- Availability: All legitimate entities should experience correct access to ATM facilities.

A threat is a potential violation of security. Threats can occur to the above identified main security objectives (confidentiality, data integrity, accountability and availability). There are several categories of threats:

- An accidental threat is a threat whose origin does not involve any malicious intent;
- An administrative threat arises from a lack of administration of security;
- Intentional threats involve a malicious entity which may attack either the communication itself or network resources.

Accidential and administrative threats usually can be avoided with the same measures used to protect against intentional threats. Most problematic are intentional threats, which can be categorized as:

- ❒ Masquerade ("spoofing"): The pretense by an entity to be a different entity;
- ❒ Eavesdropping: A breach of confidentiality by monitoring communication;
- ❒ Unauthorized access: An entity attempts to access data in violation to the security policy in force;
- ❒ Loss or corruption of information: The integrity of data transferred is compromised by unauthorized deletion, insertion, modification, reordering, replay or delay;
- ❒ Repudiation: An entity involved in a communication exchange subsequently denies the fact;
- ❒ Forgery: An entity fabricates information and claims that such information was received from another entity or sent to another entity;
- ❒ Denial of Service: This occurs when an entity fails to perform its function or prevents other entities from performing their functions. This may include denial of access to ATM services and denial of communication by flooding the ATM network/component. In a shared network, this threat can be recognized as a fabrication of extra traffic that floods the network, preventing others from using the network or delaying the traffic of others.

Not every threat is dangerous for the various security objectives. The following figure illustrates the relationship between the types of threats and the security objectives.

Main Security Objectives	Generic Threats						
	Masquerade	Eavesdropping	Unauthorized Access	Loss or Corruption of (transferred) Information	Repudiation	Forgery	Denial of Service
Confidentiality	x	x	x				
Data Integrity	x		x	x		x	
Accountability	x		x		x	x	
Availability	x		x	x			x

Figure 12.1: Mapping of security objectives and intentional threats

A set of principal security requirements have been identified to handle these threats. In addition their corresponding security services have been defined. These functional security requirements are valid for all networks, and they have been transferred to ATM specific security requirements, which are referred to as AF SEC-1 to AF SEC-10. Figure 12.2 gives an overview of the mapping between security requirements, the security service, and the ATM terminology.

Functional Security Requirement		Security Service	ATM specific
Verification of Identities		User Authentication Peer Entity Authentication Data Origin Authentication	AF SEC-1
Controlled Access and Authorization		Access Control	AF SEC-2
Protection of Confidentiality	Stored Data	Access Control	AF SEC-3
	Transferred Data	Confidentiality	
Protection of Data Integrity	Stored Data	Access Control	AF SEC-4
	Transferred Data	Integrity	
Strong Accountability		Non Repudiation	AF SEC-5
Activity Logging		Security Alarm, Audit Trail and Recovery	AF SEC-6
Alarm Reporting		Security Alarm, Audit Trail and Recovery	AF SEC-7
Audit		Security Alarm, Audit Trail and Recovery	AF SEC-8
Security Recovery /		-	AF SEC-9
Management of Security			AF SEC-10

Figure 12.2: Functional security requirements, security services and ATM terminology

12.2 ATM Security Services

In the past the security issues were often handled with various ad hoc measures to protect the network against a specific threat. Often the necessary security service was added to the already existing and developed network. The result was a variety of various solutions for different requirements. A secure network architecture is necessary for ATM networks, as well as for all other networks. The goal for a future ATM solution is an homogeneous security architecture. This architecture is based on the reference model for the B-ISDN protocol stack. In this model the different functions for data transfer, network control and network management are identified in three protocol planes:

- User plane;
- Control plane and
- Management plane.

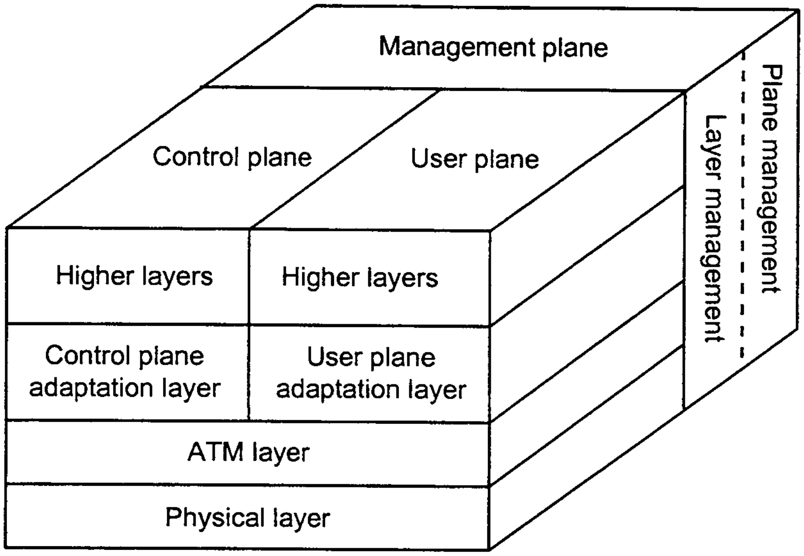


Figure 12.3: B-ISDN reference model

Most security systems focus on protection against a specific threat or for a specific network type. The security architecture should be based on the B-ISDN reference model to support interoperability and should protect the user plane, the control plane, and the management plane in an ATM network. Providing security is not so easy in ATM networks as it is in other network because of the high-speed cell relay nature of ATM:

- The flexible bandwidth allocation with a range from a few Mbit/s to Gbit/s in ATM networks require a security system that current solutions do not support. Most of the traditional crypto mechanisms work up to a several Mbit/s (with software implementation) and up to a few hundred Mbit/s (with hardware implementation).
- Another problem in selecting an efficient crypto mechanism is the small ATM cell size with a payload of only 48 bytes. The result is a restricted block cipher that operates on block size less than 384 bits.
- Even though ATM networks with very low BER channels would lose only very few cells, the loss of data can imply the loss of synchronization, and synchronization is a necessity for an encrypted data stream.

On the other hand, this cell-based structure allows the designer of high speed crypto-systems to perform security operations at various levels:

- Cell stream level with both header and user payload protection;
- Cell stream level with user payload protection;
- Per-virtual circuit (VC) level with user payload protection.

User plane security:

User plane security services provide protection for user information carried over virtual connections in a number of ways, and include the following:

- ❒ Authentication: allows the calling and called parties to positively identify each other such that a third party cannot impersonate either one of the two (e.g., spoofing or masquerade);

- Confidentiality: provides protection against third-party “eavesdropping” of the data sent on the virtual connection;
- Integrity: provides assurance that the data carried by the virtual connection cannot be modified by a third-party;
- Access Control: provides additional security-related information which, at the time of connection establishment, allows the endpoints to determine whether to accept the connection request according to the site security policy;
- Key exchange: allows the calling and called parties to agree on keys which will be used during the lifetime to the virtual connection to provide data integrity and confidentiality services;
- Security message exchange protocols: provide an optional mutual authentication and an optional one- or two-way key exchange; the three-way security message exchange protocol supports negotiation of security services and options, and optional certificate exchange.

Data confidentiality and data origin authentication are measures to protect the user plane against threats. Data confidentiality can be provided by encryption of sensitive data such that only the intended parties may decipher them correctly. Data origin authentication can be provided by using a Message Authentication Code.

As mentioned in the last section it is necessary to beware of the loss of synchronization. A synchronization loss can be avoided by inserting synchronization points into the ATM data stream. Approaches for inserting these points are based on the following techniques:

- Periodic: insertion of synchronization points at periodic intervals;
- Encapsulation: encapsulation of a synchronised block within the AAL unit;
- PDU boundaries: integrity check at suitable PDU boundaries, so that the application can efficiently discard corrupted data units.

All approaches have pros and cons. A periodic insertion is only recommended for CBR traffic, not for VBR or ABR. If encapsulation is used with an AAL5, a synchronization block can exceed the 64k bytes frame lengths and fragmentation is necessary. The approach using PDU boundaries violates against the principle that lower layers should not be required to understand higher layer structures. The conclusion is that the preferred method is always a combination of periodic insertion and insertion at PDU boundaries.

Control plane security services:

Control plane security services provide security protection mechanisms for the ATM signaling infrastructure. Only authentication has been defined as a security service for the control plane, which means that it provides strong protection against spoofing. The following approaches have been investigated:

- Security measures for signaling: offers a security signaling and a signaling security;
- Network control model: approach to separate the control function into a coherent external system;
- Key management protocol: use of response protocol, authentication protocol (e.g., X.509) or station-to-station protocol;

- MSN-CMA signaling protocol security: extension of security features to the Multi-Service Network Connection Management Architecture (MSN-CMA).

Management plane security services:

Not a lot of work has been done in this area. Although management plane security services definitions are not ready, a few approaches to support security services for the managment plane exist:

- Authenticated neighbour discovery: use of a special protocol to get information about the network neighbours;
- ILMI security: ILMI security functions can be enhanced with the use of the SNMP security protocol;
- PVC security: allows the network management to use security features in case of a PVC setup;
- VPI security: depends on the required kind of protection.

Common to all security services in these three planes, it is necessary to exchange security messages. The messaging mechanism used by the security services varies, depending on whether the service is invoked during or after connection establishment. The following methods are possible for a security messaging after connection establishment:

- Security Signaling: extension of security features to existing ATM signaling specifications (e.g., P-NNI, B-ICI);
- In-band security messaging: exchanges the security information elements in the user data channel immediately after it is established and before user data traffic begins.

Future ATM network security will provide protection for both user information and network infrastructure. A lot of work has to be done in the future. For an interoperable and flexible network architecture, the network security concept should be based on the ATM Forum Security Specification to be described in the next section.

12.3 ATM Forum Security Specification

12.3.1 General Discussion

The ATM Forum Technical Committee is working on a security specification for ATM networks. The specification is still in draft form and should define a security architecture which is interoperable to many other network and security specifications.

The aims of the ATM Forum Security Specification (ATMF SEC) are:

- Support multiple specification-defined algorithms and key lengths;
- Define a security infrastructure which provides interoperability among vendors supporting one or more of the algorithms defined in the ATMF SEC;
- Define a security infrastructure which provides for negotiation of private algorithms not specified in the ATMF SEC;
- Maintain compatibility with devices that do not implement the security extensions;
- Minimize the impact on other specifications;
- Maintain compatibility across successive versions of the ATMF SEC;
- Define mechanisms which will scale to a large (potentially global) number of users;
- Define mechanisms which provide separability of authentication and integrity from confidentiality.

The ATMF SEC describes security mechanisms (authentication, confidentiality, data integrity, and access control) for three planes in the B-ISDN reference model:

- User plane: provides transfer of user data across ATM VCCs and VPCs;
- Control plane: deals with connection establishment, release, and other connection functions, including UNI, NNI and ICI signaling;
- Management plane: performs management and coordination functions related to both the user and the control plane (including the PNNI functions related to the establishment of a routing infrastructure).

Each plane consists of three or more protocol layers: the physical layer, the ATM layer, the AAL and the upper layers if required. The current draft specification does not cover all scopes of ATM security. Figure 12.4 illustrates the areas that were defined:

	User Plane	Control Plane	Management Plane
Authentication	X	X	
Confidentiality	X		
Data Integrity	X		
Access Control	X		

Figure 12.4: Scope of ATMF SEC (draft)

The AMTF SEC (Version 1.0) deals with the security for three different scenarios: user-to-user, user-to-network, and network-to-network (Fig. 12.5).

PLANE	END-TO-END	SWITCH-TO-SWITCH	END-TO-SWITCH
User	Authentication Confidentiality Integrity	Authentication Confidentiality	Not defined
Control	Authentication	Authentication	Authentication
Management	Authentication	Authentication	Authentication

Figure 12.5: Security types in ATMF SEC Version 1.0

Compliance for an ATM security implementation is specified in terms of security service and security message exchange profiles. The security service profiles are specified in terms of specific algorithms for each of the four ATM security services areas:

1. User plane authentication, key exchange and key update (AUTH);
2. User plane confidentiality (CONF);
3. User plane data origin authentication and integrity (INTEG);
4. User plane access control (ACC).

Figure 12.6 describes the ATM security service profiles and the algorithms required to support a specific security service. The algorithms used are:

CBC (Cipher Block Chaining): A mode of operation for block ciphers (e.g., DES and FEAL);

CBC-MAC (CBC Message Authentication Code): A mechanism to provide message integrity and authenticity that uses a block cipher in CBC mode;

DES (Data Encryption Standard): A U.S. standard (published by NIST) for data encryption;

DES40: DES with a forty-bit effective key;

DSA (Digital Signature Algorithm): The algorithm specified by the DSS;

DSS (Digital Signature Standard): A U.S. standard (published by NIST) for digital signatures;

ECB (Electronic Code Book): A mode of operation for block ciphers (e.g., DES and FEAL);

ECC (Elliptic Curve Cryptosystem): A cryptosystem for digital signatures and key exchange;

ESIGN (Efficient digital SIGNature scheme): A digital signature algorithm;

FEAL (Fast data Encipherment Algorithm): An encryption algorithm developed by NTT Corp.;

MD5 (Message Digest 5): A hash algorithm that is typically used when generating digital signatures;

NIST (National Institute of Standards and Technology) in U.S.;

RSA (Rivest, Shamir, and Adleman): The encryption/digital signature algorithm invented by Rivest, Shamir, and Adleman;

SHA (Secure Hash Algorithm): The hash algorithm specified by the DSS.

ATM Security Profile	Security Service	Algorithms
AUTH-1	User Plane Authentication Key Exchange Key Update	DES/CBC DES/CBC MD5
AUTH-2	User Plane Authentication Key Exchange Key Update	DES40/CBC DES40/CBC MD5
AUTH-3	User Plane Authentication Key Exchange Key Update	DES/SHA Diffie-Hellmann SHA
AUTH-4	User Plane Authentication Key Exchange Key Update	Elliptic-Curve/DSA Elliptic-Curve/Diffie-Hellmann MD5
AUTH-5	User Plane Authentication Key Exchange Key Update	ESIGN Diffie-Hellmann MD5
AUTH-6	User Plane Authentication Key Exchange Key Update	FEAL/CBC FEAL/CBC MD5
AUTH-7	User Plane Authentication Key Exchange Key Update	RSA/MD5 RSA MD5
CONF-1	User Plane Confidentiality	DES/CBC and ECB
CONF-2	User Plane Confidentiality	DES/Counter and ECB
CONF-3	User Plane Confidentiality	DES40/CBC and ECB
CONF-4	User Plane Confidentiality	DES40/Counter and ECB
CONF-5	User Plane Confidentiality	FEAL/CBC and ECB
CONF-6	User Plane Confidentiality	FEAL/Counter and ECB
CONF-7	User Plane Confidentiality	Triple DES/CBC and ECB
CONF-8	User Plane Confidentiality	Triple DES/Counter and ECB
INTEG-1	User Plane Integrity	DES/CBC
INTEG-2	User Plane Integrity	FEAL/CBC
INTEG-3	User Plane Integrity	Keyed MD5
ACC-1	User Plane Access Control	Standard Security Label

Figure 12.6: ATM security service profiles

The second part of the compliance specification defines the security message exchange (SME) profiles and three ATM security messaging mechanisms:

- ❒ SME-1: In-band security messaging;
- ❒ SME-2: Signaling-based security two-way messaging, with a fall-back to in-band security messaging;
- ❒ SME-3: Signaling-based security three-way messaging, with a fall-back to in-band security messaging.

12.3.2 Reference Models

The functionality of the ATMF SEC is described through two reference models. The first is an object model that represents the entities within a single ATM network element involved in specific instances of security services. The second shows the interfaces and interactions among ATM network elements that are needed to support security service instances.

12.3.2.1 ATM Network Element Object Model

This model is based on the ATM protocol reference model consisting of the user plane, the control plane, and the management plane.

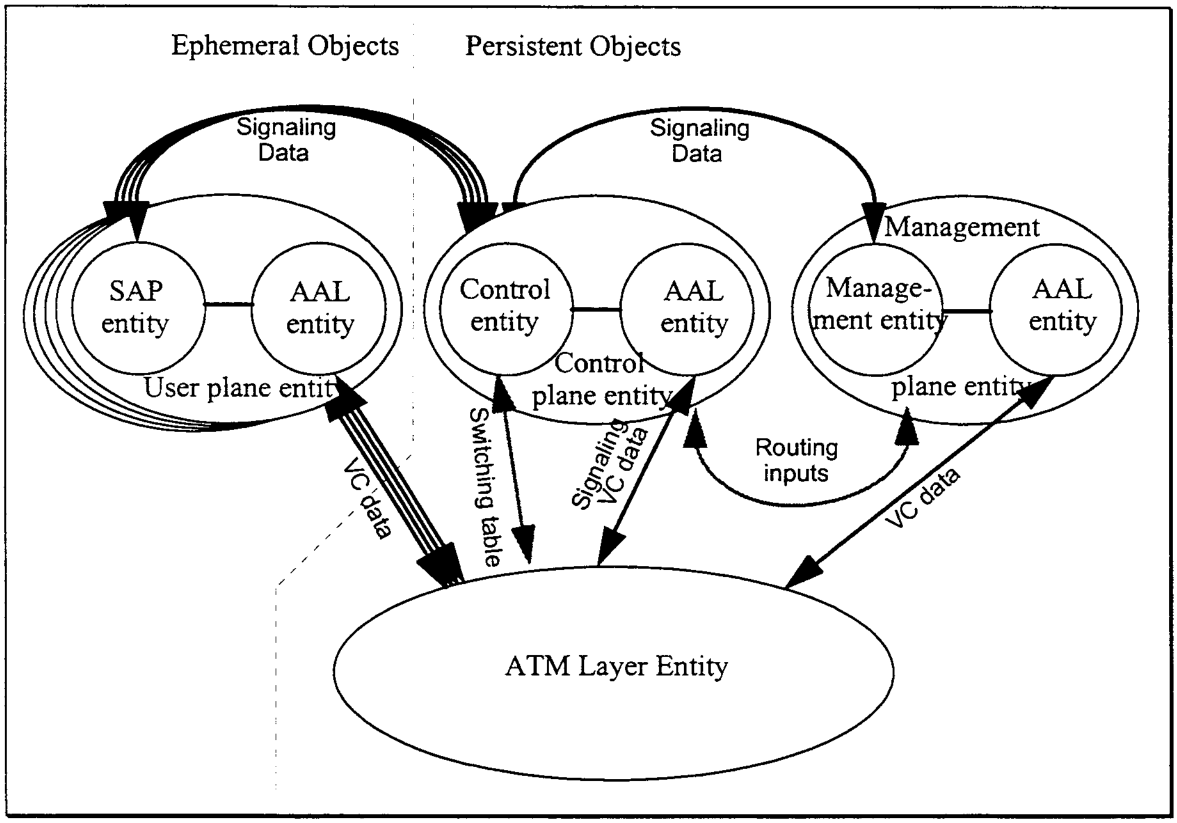


Figure 12.7: ATM network element object model

The specification describes the entities of this model (for all three planes) in terms of:

- The function of the entity;
- The lifespan of the entity (time from creation to demise);
- The contained entities and
- The interactions with other Object Model entities.

12.3.2.2 ATM Security Interactions and Interfaces Reference Model

The ATM Security Interactions and Interfaces Reference Model shows how ATM network elements interact to provide the various ATM layer security services at various interfaces, e.g., endpoint-to-endpoint (user-to-user), endpoint-to-network element (user-to-network) or network element-to-network element (network-to-network).

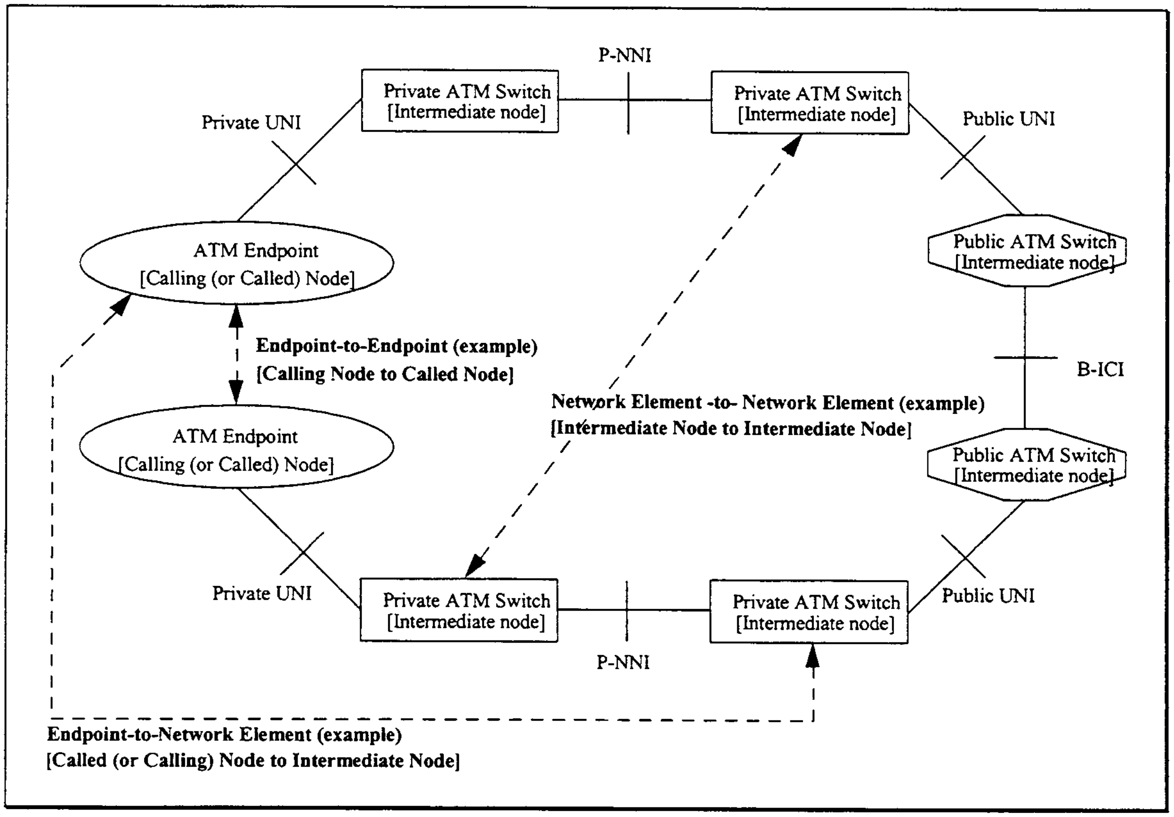


Figure 12.8: ATM security interfaces and interactions reference model

12.3.3 ATM Security Services

The objective of ATMF SEC (phase I) is to define the security services for the user plane and the control plane. The user plane security services are provided to point-to-point and point-to-multipoint SVCs as well as PVCs.

The user plane security services are:

- Authentication;
- Data confidentiality;
- Data integrity and
- Access control.

Additional support services have been defined for the user plane:

- Security message exchange and negotiation of security options;
- Key exchange;
- Key update and
- Certification infrastructure.

The only security service defined for the control plane so far is authentication.

12.3.3.1 Security Services for the User Plane

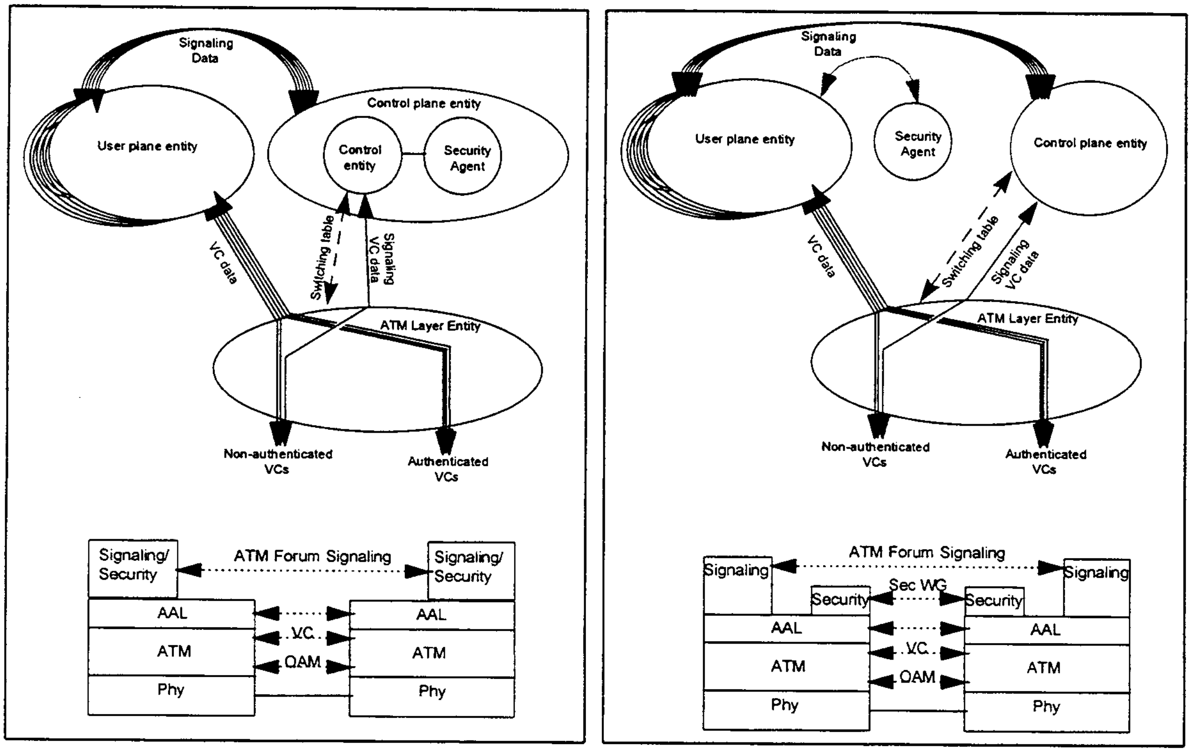
12.3.3.1.1 Authentication

The first step in establishing a secure communication is entity authentication. At the beginning of the connection, one node verifies the identity of another node. A cryptograhic technique, usually either a symmetric key algorithm (e.g., DES) or an asymmetric key algorithm (e.g., RSA), is used to verify the authentication. Authentication is provided via an exchange of bi-directional or unidirectional information. It is a process to prove that only security agents are associated with the user plane entities terminating the ATM virtual path or channel. It is recommended that ATM authentication should be provided on a per-VC basis; that is:

- The decision of whether to authenticate is determined on a VC-by-VC basis;
- Authentication is performed once for a connection, during the connection establishment phase.

There are two ways for negotiating security services: signaling-based messaging and inband security messaging. As a result, two reference models have been defined to explain how the authentication is provided (Fig. 12.9), although the difference between them is small. In the case of signaling-based messaging (Fig 12.9a), the security agent is logically part of the control plane entity, whereas for the inband case, the security agent is out of the control plane (Fig. 12.9b).

Authentication is provided via an authentication protocol (called security message exchange protocol) and an authentication algorithm consisting of a digital signature and a hash function.



(a) for signaling-based messaging (b) for inband security messaging

Figure 12.9: Object and layer reference model for authentication

12.3.3.1.2 Confidentiality

User plane confidentiality protects user information carried over an ATM connection from unauthorized disclosure. Confidentiality can be accomplished by using either symmetric or asymmetric algorithms. User plane confidentiality is defined for two scenarios:

- User to user (or "endpoint-to-endpoint") and
- Network to network (or "network element-to-network element").

Confidentiality requires a cryptograghic algorithm, and is on a per-VC basis; that is,

- Encryption is applied to the sequence of data cells in a single VC;
- The decision of whether to encrypt is determined on a VC-by-VC basis;
- For encrypted VCs, encryption parameters are determined (and may vary) on a VC-by-VC basis.

Similar to the authentication model, there are two different methods for negotiating security services: signaling-based and inband security. As a result, two reference models (Fig. 12.10 and Fig. 12.11) for confidentiality have been defined. Again, the two models differ mainly in where the security agent is located.

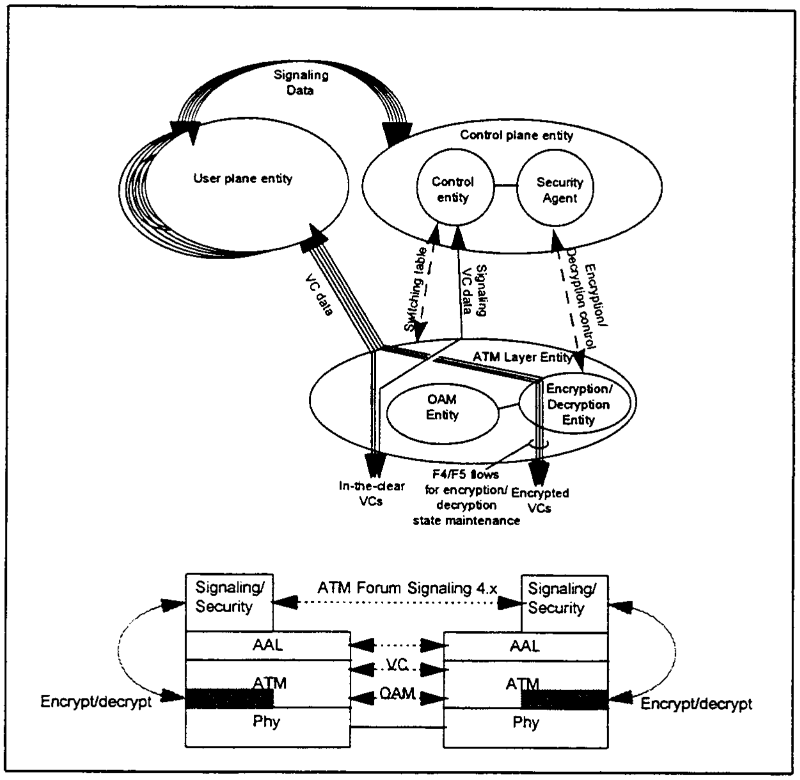


Figure 12.10: Object and layer reference model for confidentiality, (signaling-based messaging)

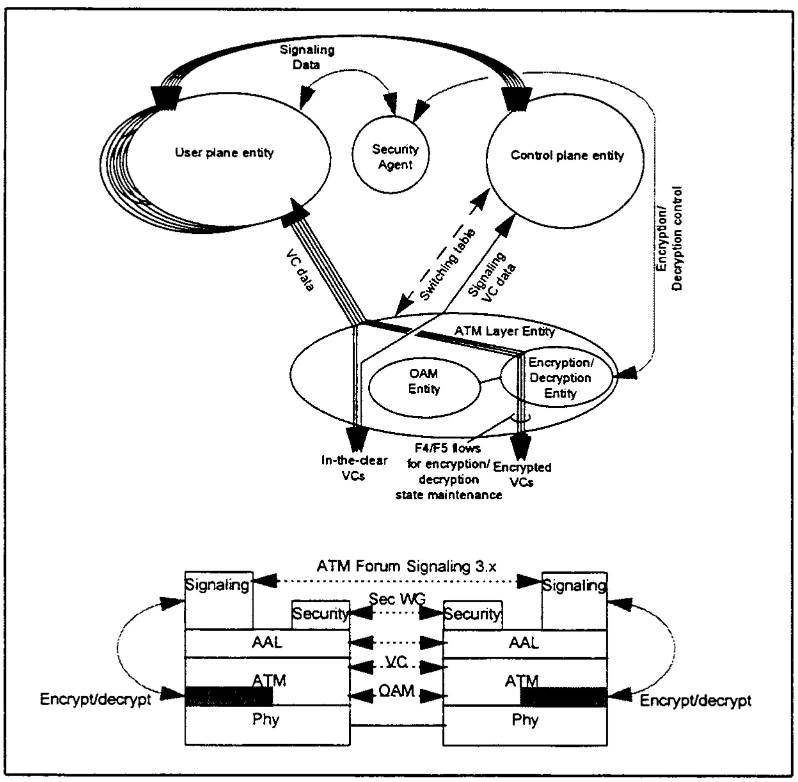


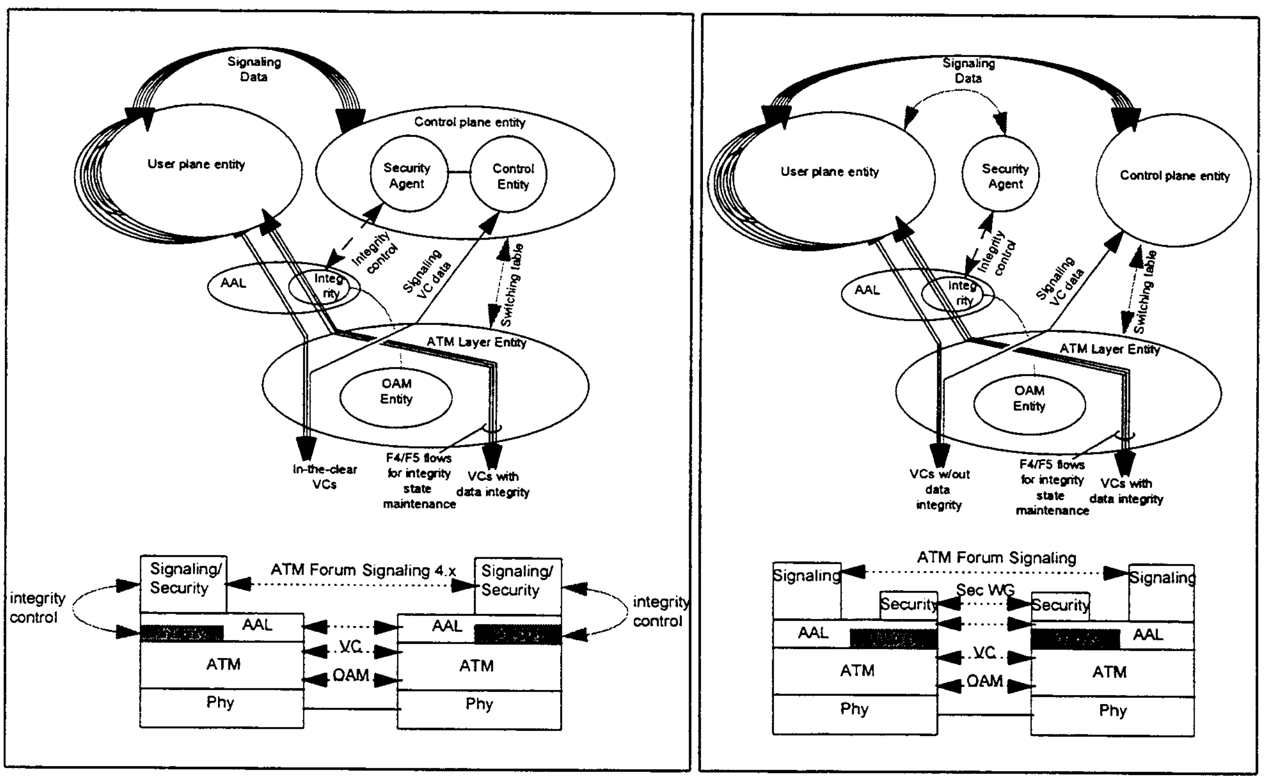
Figure 12.11: Object and layer reference model for confidentiality, (inband security messaging)

12.3.3.1.3 Data Origin Authentication and Integrity

Security service data integrity (also known as data origin authentication) guarantees that modifications to data will be detected. Data integrity requires the use of cryptographic mechanisms. Usually a cryptographic signature is added to each data unit. The signature algorithm used is a message authentication code. Service data integrity service can only be maintained for virtual channels, not virtual paths. As a consequence:

- Integrity protections do not apply to VPCs;
- Checksums are applied to the sequence of SDUs in a VCC;
- The decision of whether to provide integrity is determined on a VCC-by-VCC basis;
- For VCCs with checksums, integrity keys are determined (and may vary) on a VCC-by-VCC basis.

Again, data integrity service can be provided through signaling-based messaging and inband security messaging. The main difference of the two messaging approaches is the location of the security agent, as illustrated in their corresponding reference models (Fig. 12.12a and 12.12b).



(a) for signaling-based messaging (b) for inband security messaging

Figure 12.12: Object and layer reference model for data integrity

12.3.3.1.4 Access Control

Access control refers to the application of a set of rules to a service request. User plane access control requires mechanisms to transport access control information during connection establishment and to determine whether access to the connection should be granted. It is defined for each ATM interface (end-point-to-switch and switch-to-switch) and provided on a per VC basis. The access control service can be negotiated through either signaling-based messaging or inband security messaging. Two reference models have been defined (Fig. 12.13 and Fig. 12.14), and, again, they differ mainly in the location of the security agent. In the signaling-based messaging model, the security agent is part of the control plane entity, whereas in the inband case the security agent is not part of the control plane entity.

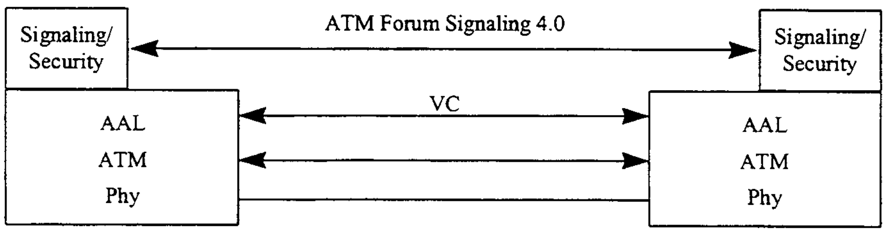


Figure 12.13: Access control layer reference model: for signaling-based messaging

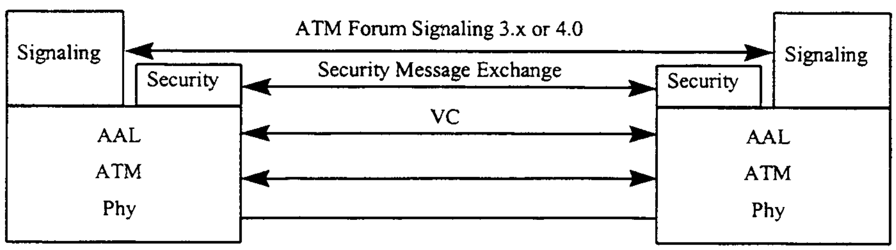


Figure 12.14: Access control layer reference model: for inband-based messaging

12.3.3.2 Security Services for the Control Plane

Authentication, which binds an ATM signaling message to its source, is the only security service defined for the control plane so far. The ATM Forum Security Working Group continues to define additional security features (e.g., digital signature) that are necessary to protect a network against most threats. These features are expected to appear in an upcoming version of security specification.

12.4 Products and Projects

Security in ATM networks is still in an infancy stage, and research studies are going on. This paragraph describes a few commercially available products and research projects.

12.4.1 Key Agile ATM Encryption Systems

Using key agile ATM encryption systems, the Defense Advance Research Projects Agency (DARPA) develops a system for a full duplex operation in an ATM network at OC-12c rate (622 Mbit/s). Up to 65,534 active connections can be supported, with each connection encrypted using a unique key. A Gbit/s DES chip is used for the data encrytion. Keys are generated and distributed among crypto units using RSA public key encryption, certificates, and digital signatures. The system should be completely transparent to the ATM network and to end user equipment at the physical layer and the ATM layer. The project also investigates issues concerning the secure communication over public ATM networks.

Most of the development in ATM encryption systems has been done by MCNC (Microelectronics Center of North Carolina) and Secant Network Technologies (SNT) in their product CellCase. The CellCase system, developed by SNT with specifications for 45 Mbit/s, 155 Mbit/s or 622 Mbit/s, offers a solution for secure ATM networking. It uses an approach that interconnects two or more trusted network islands into one virtual trusted network.

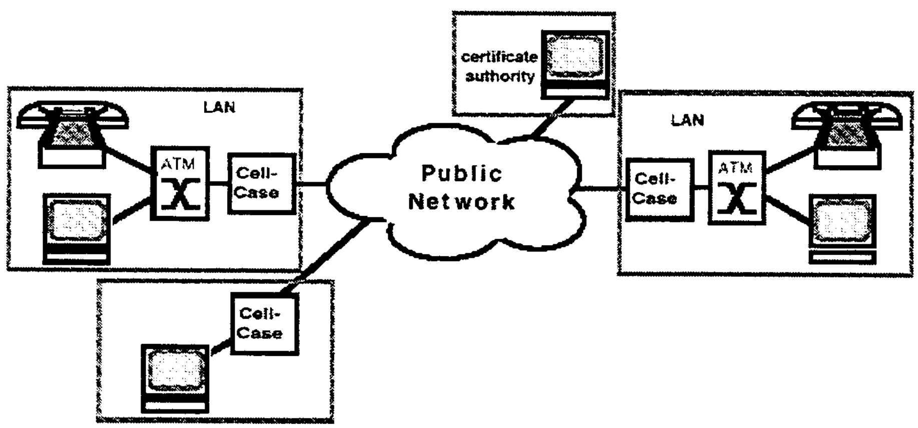


Figure 12.15: Virtual trusted networks with CellCase

12.4.2 Products from GTE

GTE offers the following products to support a security service in ATM networks:

- InfoGuard 100 ATM Cell Encruptor;
- Fastlane ATM Encryptor (KG-75) and
- Taclane.

InfoGuard 100 ATM Cell Encryptor is a commercial device that supports the encryption of ATM traffic up to 45 Mbit/s with the full advantage of ATM variable bandwidth allocation. The DES algorithm is used for data encryption, and Diffie-Hellmann is used for public key management. It is possible to use InfoGuard for

- Network operations;
- OC-3 configuration;

- Four Site Ring Configuration;
- Secure and non-secure network connectivity configuration and
- Multimedia applications configuration.

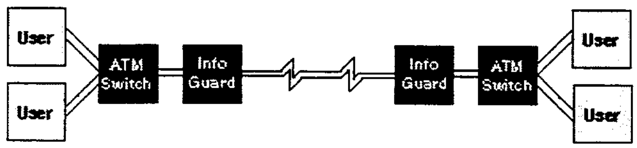


Figure 12.16: InfoGuard for network operation (as example)

The Fastlane ATM Encryptor (KG-75) provides high-speed (DS1, DS3, OC-3c and OC-12), transparent, low-latency security for multi-media applications in a point-to-point or point-to-multipoint connection. Since KG-75 is approved as DoD type 1 security system up to TS/SCI by the NSA, it is possible to use Fastlane in a military environment.

The Taclane is a MISSI In-Line Network Encryptor, and provides NSA-approved security in Ethernet and ATM networks. When used as ATM encryptor, Taclane should provide low-speed ATM cell security, and is interoperable to the Fastlane ATM Encryptor.

12.4.3 Products from Motorola

Motorola´s Space and Systems Technology Group offers the following security products:

- KG-189;
- KG-95 and
- KGV-135.

KG-189 is a SONET-compatible encryptor for OC-3, OC-12 and OC-48 rates. It fulfils the NSA Tempest Specification and can be used in a military environment. KG-95 is a trunk encryption device for either a fixed DS-3 rate or variable rate between 10 and 50 Mbit/s. It can be used in a full duplex operation, and meets the military standards MIL-STD-188-114A. KGV-135 is a high-speed KG module, which can be used for wideband operations from 2 kbit/s to 700 Mbit/s. NSA-approved cryptography can be used in the KGV-135.

13 ATM-Testing

13.1 Test Suites

Many standards have been developed for the ATM technology. The ATM Forum and the IETF have defined specifications for most multimedia applications used in ATM networks. There must be a means for a user to determine whether an ATM product is compliant with ATM-based specitication. As a result, the ATM Forum has developed specifications and processes that can be used to test ATM products. Two main documents, referred to as “pro formas”, have been defined by the Forum for conformance testing:

- PICS (Protocol Information Conformance Testing Statement) and
- PIXIT (Protocol Implementation Extra Information for Testing).

The PICS associated with an ATM product identifies the standard-based specification protocol options that were implemented. PIXIT contains additional information such as features not identified in a specification or means to configure a product for testing.

PICS and PIXIT will facilitate the testing of ATM products.

13.2 Test Specifications

Much work has been done to define performance measurements and test methods. The ATM Forum has defined many PICSs for the various implementations. The ITU-T Recommendation I.356 defines ways to measure the speed, accuracy and dependability of end-to-end cell transfer at the ATM layer.

13.3 Ways to do Testing

There are three categories of testing:

- Conformance;
- Interoperability and
- Performance.

Conformance refers to whether a product is compliant with a standard-based specification. Interoperability refers to whether a product can work with other systems to perform a common function. Performance refers to how well a product can perform a function. Conformance testing precedes the other two categories of testing. There are two categories of conformance testing:

- Static and
- Dynamic.

Static conformance testing involves no actual testing at all and merely checks against a PICS to determine which protocol options in a specification have been implemented. Dynamic testing involves actual tests and checks whether every mandatory protocol option of a specification has been implemented correctly. Figure 13.1 illustrates the steps involved in conformance testing.

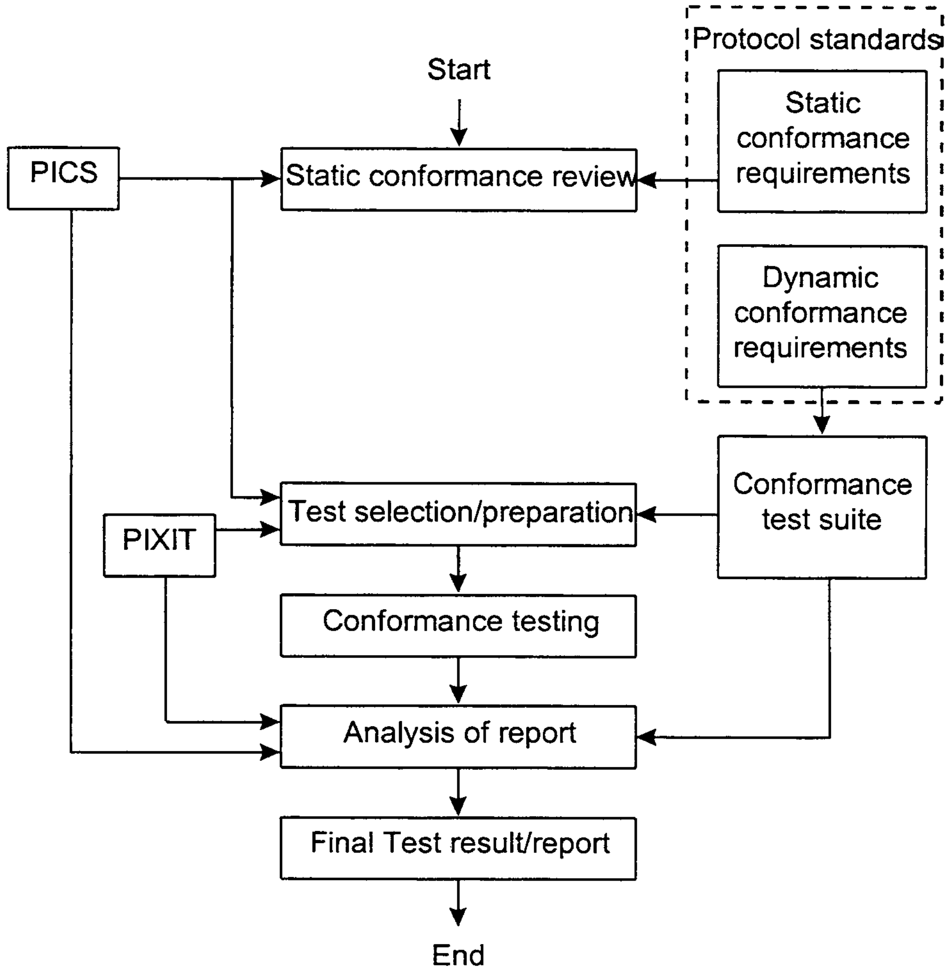


Figure 13.1: Outlining Conformance

Because a specification has both mandatory and optional parameters, it is entirely possible that two conforming products cannot interoperate. Figure 13.2 shows the steps involve in interoperability testing. Performance testing determines how well a product can perform a function. The ATM Forum has yet to complete a specification providing guidelines for performance testing.

The sequence of steps taken to perform a test is referred to as a test procedure. There are two categories of test procedure:

- The abstract test suite and
- The executable test suite.

An abstract test procedure describes a test in an equipment-independent way, and an executable test procedure describes a test using equipment-specific instructions. An executable test procedure is typically specified in terms of computer code developed by test product vendors.

So far relatively few testing guidelines have been provided by the ATM Forum; however, it is expected that testing guidelines involving traffic management policies will be developed soon.

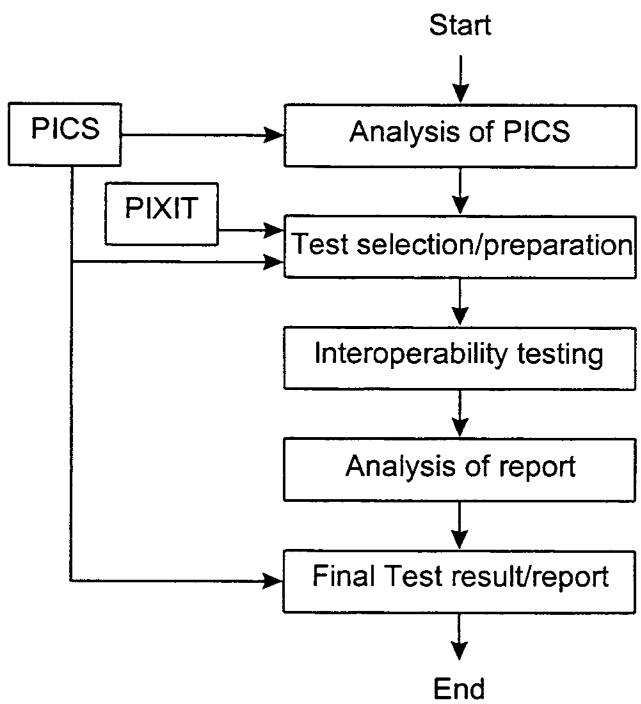


Figure 13.2: Testing Interoperability

13.4 Test Cell

Test cells may be used to determine whether the requested QoS of a user is indeed satisfactory. The ATM Forum Testing Working Group is finalizing a standard means (similar to that specified in the ITU-T Recommendation O.191) to generate and monitor ATM test cells so that performance parameters such as CLR, CMR, and CER of connections can be measured. A test cell (Fig. 13.3), generated onto a virtual connection by a test equipment, contains a 48-byte payload with a CRC, a timestamp, and a sequence number. The high-resolution (10ns) timestamp permits the measurement of end-to-end delay and CDV. The 16-bit CRC and sequence number allows the detection of lost and errored cells.

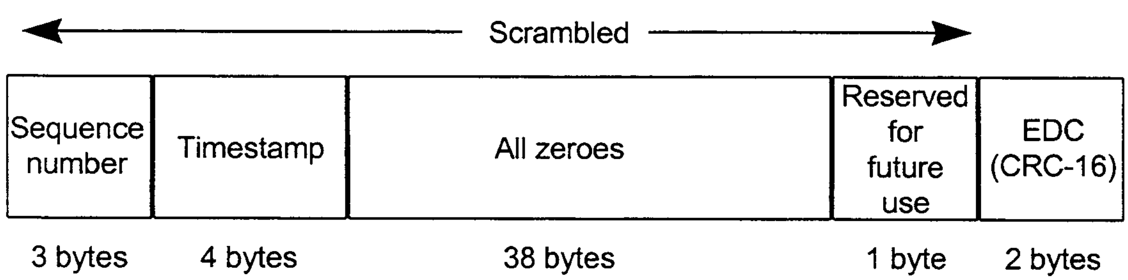


Figure 13.3: Test cell

13.5 Test Support

It is not necessary to test each ATM equipment used in a system. Many ATM products have been tested by various companies and organizations, and the test results are maintained by the Joint Interoperability Test Command (JITC) ATM Testing, a part of the Defense Information Systems Agency (DISA).

14 Trends in ATM Implementations (European and US Market)

ATM products are being used in three communication segments:

- Public Network Infrastructure;
- Local Area Networks (LAN) and
- Wide Area Networks (WAN).

The markets are different in these three segments.

14.1 Public Network Infrastructure

In Europe, telecommunication service and networks are regulated by the European Union (EU) and by individual state governments. These regulations supports interoperability between different providers. The PTTs in Europe are monopolies, and the main EU telecommunication policy is to separate services from the infrastructure. Other data services or mobile telephonies (cell-phone) are fully deregulated and offered by various companies. The governments issue only the licenses to build up the service. All providers have to use the infrastructure provided through Open Network Provisions (ONPs). ONPs are requirements that define the available connections and interfaces. The major differences in infrastructure markets between Europe and the U.S. are:

- The regulatory environment: In Europe, there is a separation between service and infrastructure.
- The procurement environment: A requirement for public utilities to use the ETSI standards.
- The political environment: Initiatives for a super data-highway only in a few countries.

For the future, the European market will be more liberalized, as in the U.S., so that many carriers can offer ATM-based products and services.

14.2 ATM LANs

Local Area Networks have been developed to interconnect personal computers. Today's LANs are used also for interconnecting workstations and other computer resources over a relatively short distance.

The LAN market is the fastest changing segment. Typically, Europe is 12 to 18 months behind the U.S. in offering newer LAN technologies, and there are only a few differences in the LAN technologies used in the U.S. and in Europe. Some of these differences are WAN interfaces, electro-magnetic compatibility regulations (much more stringent in Europe), and market fragmentation. The fragmentation is a result of the many regulations and requirements in Europe, and prevents expansions of the technologies. Consequently, most LAN technologies are developed in the U.S.

14.3 ATM WANs

Since WANs cover large geographic areas and span many users and equipment, the costs of designing, building, and maintaining these networks are enormous. Efficient use of resources is paramount for these networks. ATM offers efficient support for existing data and real-time application services. Indeed, ATM is the only technology that can support diverse applications over a wide area.

There are several important differences between the U.S. and European ATM WAN markets. In the U.S., the physical interface rates used are 1.5 Mbit/s and 45 Mbit/s, whereas in Europe, 2 Mbit/s and 34 Mbit/s interfaces are used. Lower rates are used in Europe because a leased line is much more expensive there. As a result, the most commonly used connections are 64 kbit/s and E1. Both regions have essentially the same services. Frame Relay, which offers data services up to 2 Mbit/s, is more popular in the U.S. Much slower data services, offered by X.25 networks, are used in Europe.

15 Summary

The last fourteen chapters summarize the ATM technology as of today, but research and development on ATM are still ongoing worldwide. The complexity and the many rapid changes of ATM make it difficult for scientists to keep track with this technology. The ATM Forum alone has twelve working groups designing specifications. Although originally conceived as a broadband WAN technology, ATM has also been shown to be a feasible architecture for the local area environments. This, combined with the application-independent advantage of ATM, makes ATM a likely technology for providing a seamless communication infrastructure worldwide. It is expected that ATM will replace or interoperate with most of today's WANs, MANs, and LANs. Although a decade had passed since ATM was selected as the transfer mode for B-ISDN, it will take perhaps another ten years before ATM can become widely deplored and fulfil its promise as the unifying technology that supports all applications.

ATM is designed based on the assumptions that high-speed and low-error-rate channels are available. Since the channels used in military environment tend to be very low grade, why would one consider using ATM in such an environment?

Although the results are preliminary in nature, investigations in the past few years demonstrate that it may be useful to integrate ATM into military communication systems. It is especially important because this COTS technology can reduce costs, improve system requirements and interoperate with most of the networks used today. The possible use of ATM has not been limited to the Navy C^4I-systems (Command, Control, Communications, Computer and Intelligence); the armed forces of the U.S. and of several European countries have been developing and investigating ATM to use as integrated network. New areas, such as wireless ATM, will impact the design of future systems and offer more flexibility than current ATM technology.

Many problems (e.g., network security) have to be solved. Code D827 is working on solutions to meet the military requirements of JMCOMS (Joint Maritime Communication System) to realize modern C^4I-systems for the Navy. The following projects of Code D827 are examples of the many efforts on ATM at NRaD:

- MONET (High Data Rate Mobile Internet);
- JDE (JMCOMS Joint Development Environment);
- HIPNET (Multiservice Internet Protocols for High Performance Networks);
- DAWN (Demonstrator of Advanced Wireless Network).

Even though much work has been done on the subject, a rather safe conclusion that can be drawn from the many ongoing studies is that it will require considerable additional time and expenditure before ATM would become a mature technology.

16 Standards

16.1 ATM-Forum

16.1.1 Current Standards

The following approved specifications are available by the ATM Forum:

B-ICI:

- B-ICI 1.0
- B-ICI 1.1
- B-ICI 2.0 (delta spec to B-ICI 1.1)
- B-ICI 2.0 (integrated specification)
- B-ICI 2.0 (Addendum or 2.1)

Data Exchange Interface:

- Data Exchange Interface version 1.0

Integrated Local Management Interface:

- ILMI 4.0

LAN Emulation:

- LAN Emulation over ATM 1.0
- LAN Emulation Client Management Specification
- LANE 1.0 Addendum
- LANE Servers Management Spec v1.0

Network Management:

- Customer Network Management (CNM) for ATM Public Network Service
- M4 Interface Requirements and Logical MIB
- CMIP Specification for the M4 Interface
- M4 Public Network view
- M4 "NE View"
- Circuit Emulation Service Interworking Requirements, Logical and CMIP MIB
- M4 Network View CMIP MIB Spec v1.0
- M4 Network View Requirements & Logical MIB Addendum

Physical Layer:

- Issued as part of UNI 3.1: 44.736 DS3 Mbit/s Physical Layer
  100 Mbit/s Multimode Fiber Interface Physical Layer
  155.52 Mbit/s SONET STS-3c Physical Layer
  155.52 Mbit/s Physical Layer

- ATM Physical Medium Dependent Interface Specification for 155 Mbit/s over Twisted Pair Cable
- DS1 Physical Layer Specification
- Utopia Level 1 v2.01
- Mid-range Physical Layer Specification for Category 3 UTP
- 6.312 Kbit/s UNI Specification
- E3 UNI
- Utopia Level 2 v1.0
- Physical Interface Specification for 25.6 Mbit/s over Twisted Pair
- A Cell-based Transmission Convergence Sublayer for Clear Channel Interfaces
- 622.08 Mbit/s Physical Layer
- 155.52 Mbit/s Physical Layer Specification for Category 3 UTP (See also UNI 3.1)
- 120 Ohm Addendum to ATM PMD Interface Spec for 155 Mbit/s over TP
- DS3 Physical Layer Interface Spec
- 155 Mbit/s over MMF Short Wave Length Lasers, Addendum to UNI 3.1
- WIRE (PMD to TC layers)
- E-1

P-NNI:

- Interim Inter-Switch Signaling Protocol
- P-NNI V1.0
- P-NNI 1.0 Abbendum (soft PVC MIB)
- P-NNI ABR Addendum

Service Aspects and Applications:

- Frame UNI
- Circuit Emulation
- Native ATM Services: Semantic Description
- Audio/Visual Multimedia Services: Video on Demand Specification v 1.0
- Audio/Visual Multimedia Services: Video on Demand Specification v 1.1
- ATM Names Service

Signaling:

- (See UNI 3.1)
- UNI Signaling 4.0
- Signaling ABR Abbendum

Testing:

- Introduction to ATM Forum Test Specifications
- PICS Proforma for the DS3 Physical Layer Interface
- PICS Proforma for the SONET STS-3c Physical Layer Interface
- PICS Proforma for the 100 Mbit/s Multimode Fibre Physical Layer Interface
- PICS Proforma for the ATM Layer (UNI 3.0)
- Conformance Abstract Test Suite for the ATM Layer for Intermediate Systems (UNI 3.0)
- Interoperability Test Suite for the ATM Layer (UNI 3.0)
- Interoperability Test Suites for Physical Layer: DS-3, STS-3c, 100 Mbit/s MMF (TAXI)
- PICS for DS-1 Physical Layer
- Conformance Abstract Test Suite for the ATM Layer (End Systems) UNI 3.0
- PICS for AAL5 (ITU spec)
- PICS Proforma for the 51.84 Mbit/s Mid-Range PHY Layer Interface
- Conformance Abstract Test Suite for the ATM Layer of Intermediate Systems (UNI 3.1)
- PICS for the 25.6 Mbit/s over Twisted Pair Cable (UTP-3) Physical Layer
- PICS for ATM Layer (UNI 3.1)
- Conformance Abstract Test Suite for the UNI 3.1 ATM Layer of End Systems
- Conformance Abstract Test Suite of the SSCOP for UNI 3.1
- PICS for the 155 Mbit/s over Twisted Pair Cable (UTP-5/STP-5) Physical Layer

Traffic Management:

- (See UNI 3.1)
- Traffic Management 4.0
- Traffic Management ABR Abbendum

Voice and Telephony over ATM:

- Circuit Emulation Service 2.0

User-Network Interface (UNI):

- ATM User-Network Interface Specification V2.0
- ATM User-Network Interface Specification V3.0
- ATM User-Network Interface Specification V3.1
- ILMI MIB for UNI 3.0
- ILMI MIB for UNI 3.1

16.1.2 Future Standards

The following specifications will be available in the future:

B-ICI:

- B-ICI 2.2 or 3.0 (T.B.D.)

Joint PHY and RBB:

- 50 Mbit/s over Plastic Optical Fiber (POF)

LAN Emulation:

- LANE v2.0 LUNI Interface
- LANE v2.0 Server-to-server Interface

MPOA:

- MPOA v1.0

Network Management:

- ATM Remote Monitoring SNMP MIB
- Enterprise/Carrier Management Interface (M4) Requirements & Logical MIB SVC Function NE View V2.0
- Enterprise/Carrier Network Management (M4) SNMP MIB
- Carrier Interface (M5) Requirements & CMIP MIB
- Management System Network Interface Security Requirements & Logical MIB
- ATM Access Function Specification Requirements & Logical MIB

Physical Layer:

- Inverse ATM Mux
- 155 Mbit/s over Plastic Optical Fiber (POF)
- nxDS0 Interface
- 2.4 Gbit/s Interface
- 1-2.5 Gbit/s Interface
- 10 Gbit/s Interface

P-NNI (Private Network-to-Network Interface):

- Integrated PNNI (PNNI)
- Public/Private ATM Interworking
- PNNI Augmented Routing (PAR)
- PNNI v 1.0 Errata and PICs
- PNNI 2.0 (Note: includes B-QSIG PNNI interworking)

RBB (Residential Broadband):

- RBB Specification

Security:

- Security 1.0

Service Aspects & Applications:

- AMS 1.1 Addendum
- API Semantic Doc 2.0
- AMS 2.0: VBR MPEG-2 over ATM
- AMS 2.0: Multimedia Desktop
- AMS 2.0: Interworking
- FUNI 2.0

Signaling:

- Closed User Group Support, Third Party Connection, Security

Testing:

- Conformance Abstract Test Suite for Signaling (UNI 3.1) for the User Side
- Conformance Abstract Test Suite for Signaling (UNI 3.1) for the Network Side
- PICS for PNNI
- Performance Testing Specification
- PICS for Direct Mapped DS3
- SIS for LANE 1.0
- PICS for Signaling (UNI 3.1-User Side)
- Conformance Abstract Test Suite for LANE 1.0 Server
- Conformance Abstract Test Suite for UNI 3.0/3.1 ILMI Registration (User Side & Network Side)
- ATM Test Access Function (ATAF) Spec

Voice and Telephony over ATM:

- Landline Trunking
- Desktop
- Dynamic Bandwidtth CES

Wireless ATM:

- Radio Access Layer and Media Access Control Requirements Definition
- Mobility Management
- Location Management
- WATM Spec 1.0

16.2 ITU-T-Recommendations

The following specifications from the ITU-T concern the ATM network technology:

E.800	Terms and definition related to Quality of Service and Network Performance including dependability
F.812	Broadband connectionless data bearer service
G.703	Physical/electrical characteristics of hierarchical digital interfaces
G.704	Synchronous frame structures used at 1544, 6312, 2048, 8488 and 44736 kbit/s hierarchical levels
G.711	Pulse code modulation (PCM) of voice frequencies
G.726	40, 32, 24, 16 kbit/s adaptive differential pulse code modulation
G.728	Coding of speech at 16 kbit/s using low-delay code excited linear prediction
H.200	Framework for Recommendations for Audiovisual Services
H.221	Frame Structure for a 64 to 1920 kbit/s Channel in Audiovisual Teleservices
H.230	Frame-Synchronous Control and Indication Signals for Audiovisual Systems
H.261	Video Codec for Audiovisual Services at px64 kbit/s
H.320	Narrow-Band Visual Telephone Systems and Terminal Equipment
I.113	Vocabulary of terms for broadband aspects of ISDN
I.121	Broadband Aspects of ISDN
I.151	B-ISDN ATM functional characteristics
I.211	B-ISDN Service Aspects
I.311	B-ISDN General Network Aspects
I.321	B-ISDN Protocol Reference Model and its Application
I.326	Functional architecture of transport networks based on ATM
I.327	B-ISDN functional architecture
I.350	General Aspects of Quality of Service and Network Performance in Digital Networks, Including ISDNs
I.356	B-ISDN ATM layer cell transfer performance
I.361	B-ISDN ATM Layer Specification
I.362	B-ISDN ATM Adaption Layer (AAL) Functional Description
I.363	B-ISDN AAL specification
I.364	Support of Broadband Connectionless Data Service on B-ISDN
I.365	B-ISDN ATM adaptation layer sublayers
I.371	Traffic control and congestion control in B-ISDN
I.374	Framework Recommendation on Network Capabilities to Support Multimedia Services
I.413	B-ISDN User Network Interface

I.432	B-ISDN UNI-physical layer specification
I.555	Interworking
I.610	B-ISDN operation and maintenance principles and functions
I.731	Types and general characteristics of ATM equipment
I.732	Functional characteristics of ATM equipment
I.751	ATM management of the network element view
M.3010	Principles for a Telecommunications management network
Q.701	Functional description of the message transfer part (MTP) of Signaling System No. 7
Q.702	Signaling data link
Q.704	Signaling network functions and messages
Q.706	Message transfer part signaling performance
Q.707	Testing and maintenance
Q.711	Functional description of the signaling connection control part
Q.712	Definition and function of SCCP messages
Q.713	SCCP formats and codes
Q.714	Signaling connection control part procedures
Q.716	Signaling System No. 7 – Signaling connection control part (SCCP) performance
Q.721	Functional description of the Signaling System No. 7 Telephone User Part (TUP)
Q.722	General function of telephone messages and signals
Q.723	Formats and codes
Q.724	Signaling procedures
Q.725	Signaling performance in the telephone application
Q.730	ISDN supplementary services
Q.741	Signaling System No. 7 – Data user part
Q.761	Functional description of the ISDN user part of Signaling System No. 7
Q.762	General function of messages and signals of the ISDN User Part of Signaling System No. 7
Q.763	Formats and codes of the ISDN User Part of Signaling System No. 7
Q.764	ISDN user part signaling procedures
Q.766	Performance objectives in the integrated services digital network application
Q.771	Functional description of transaction capabilities
Q.772	Transaction capabilities information element definitions
Q.773	SCCP formats and codes
Q.774	Transaction capabilities procedures
Q.775	Guidelines for using transaction capabilities
Q.2100	B-ISDN signaling ATM adaptation layer (SAAL) overview description

Q.2110	B-ISDN ATM adaptation layer – Service specific connection oriented protocol
Q.2119	B-ISDN ATM adaptation layer – Convergence function for SSCOP above the frame relay core service
Q.2120	B-ISDN meta-signaling protocol
Q.2130	B-ISDN signaling ATM adaptation layer – Service specific coordination function for support of signaling at the user-network
Q.2140	B-ISDN ATM adaptation layer – Service specific coordination function for signaling at the network node interface (SSCF AT NNI)
Q.2144	B-ISDN signaling ATM adaptation layer (SAAL) – Layer management for the SAAL at the network node interface (NNI)
Q.2730	B-ISUP Supplementary Services
Q.2761	Functional Description of B-ISUP
Q.2762	General Functions of Messages and Signals of B-ISUP of SS7
Q.2763	B-ISUP Formats and Codes
Q.2764	SS7 B-ISUP Basic Call Procedures
Q.2931	B-ISDN User-Network Interface Layer 3 Specification for Basic Call/Bearer Control
Q.2932	B-ISDN signaling
X.711	Common management information protocol (CMIP) specification for ITU-T applications

16.3 ANSI

The following specifications from the ANSI concern the ATM network technology:

T1A1	Performance and signal processing
T1E1	Network interfaces and environmental considerations
T1M1	Internetwork operations, administration, maintenance, and provisioning
T1P1	Systems engineering, standards planning, and program management
T1S1	Service architecture and signaling
T1X1	Digital hierarchy and synchronization
T1.624	B-ISDN UNI: Rates and formats specification
T1.627	B-ISDN ATM functionality and specification
T1.629	B-ISDN AAL3/4 common part functionality and specification
T1.630	B-ISDN: Adaptation layer for CBR services functionality and specification
T1.633	Frame Relay bearer service interworking
T1.634	Frame Relay service specific convergence sublayer
T1.635	B-ISDN AAL type 5

16.4 RFCs

The following RFCs describe technologies which are used in ATM networks:

RFC 1112	Host extensions for IP multicasting
RFC 1155	Structure and identification of management information for TCP/IP-based internets
RFC 1157	Simple Network Management Protocol (SNMP)
RFC 1190	Experimental Internet Stream Protocol: Version 2 (ST-II)
RFC 1213	Management Information Base for network management of TCP/IP based internets
RFC 1215	Convention for defining traps for use with the SNMP
RFC 1237	Guidelines for OSI NSAP Allocation in Internet
RFC 1406	Definitions of Managed Objects for the DS1 and E1 Interface Types
RFC 1407	Definitions of Managed Objects for the DS3/E3 Interface Type
RFC 1483	Multiprotocol Encapsulation over ATM Adaptation Layer 5
RFC 1573	Evolution of the Interfaces Group of MIB-II
RFC 1577	Classical IP and ARP over ATM
RFC 1626	Default IP MTU for use over ATM AAL5
RFC 1680	IPng Support for ATM Services
RFC 1695	Definitions of Managed Objects for ATM Management Version 8.0
RFC 1705	Six Virtual Inches to the Left: The Problem with IPng
RFC 1719	A Direction for IPng
RFC 1726	Technical Criteria for Choosing IP The Next Generation (IPng)
RFC 1752	The Recommendation for the IP Next Generation Protocol
RFC 1753	IPng Technical Requirements Of the Nimrod Routing and Addressing Architecture
RFC 1754	IP over ATM Working Group's Recommendations for the ATM Forum's Multiprotocol BOF Version 1
RFC 1755	ATM Signaling Support for IP over ATM
RFC 1819	Internet Stream Protocol Version 2 (ST2) Protocol Specification
RFC 1821	Integration of Real-time Services in an IP-ATM Network Architecture
RFC 1889	RTP: A Transport Protocol for Real-Time Applications
RFC 1890	RTP Profile for Audio and Video Conferences with Minimal Control
RFC 1901	Introduction to Community-based SNMPv2
RFC 1902	Structure of Management Information for Version 2 of the SNMPv2
RFC 1903	Textual Conventions for Version 2 of the Simple Network Management Protocol (SNMPv2)

RFC 1904	Conformance Statements for Version 2 of the Simple Network Management Protocol (SNMPv2)
RFC 1905	Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2)
RFC 1906	Transport Mappings for Version 2 of the Simple Network Management Protocol (SNMPv2)
RFC 1907	Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2)
RFC 1908	Coexistence between Version 1 and Version 2 of the Internet-standard Network Management Framework
RFC 1926	An Experimental Encapsulation of IP Datagrams on Top of ATM
RFC 1932	IP over ATM: A Framework Document
RFC 1946	Native ATM Support for ST2+.
RFC 1954	Transmission of Flow Labelled IPv4 on ATM Data Links Ipsilon Version 1.0.
RFC 1955	New Scheme for Internet Routing and Addressing (ENCAPS) for IPNG
RFC 2022	Support for Multicast over UNI 3.0/3.1 based ATM Networks
RFC 2029	RTP Payload Format of Sun's CellB Video Encoding
RFC 2032	RTP Payload Format for H.261 Video Streams
RFC 2035	RTP Payload Format for JPEG-compressed Video
RFC 2038	RTP Payload Format for MPEG1/MPEG2 Video
RFC 2107	Ascend Tunnel Management Protocol - ATMP

17 Appendix

Table of Figures

18 Acronyms

AA	Administrative Authority
AAI	ACTS ATM Internetwork (in the U.S.)
AAL	ATM Adaptation Layer
AAL 1	AAL Type 1
AAL 2	AAL Type 2
AAL 3/4	AAL Type 3 and 4
AAL 5	AAL Type 5
AALPCI	AAL Protocol Control Information
AALSDU	AAL Service Data Unit
ABR	Available Bit Rate / Actual Cell Rate
ACE	Access Connection Element
ACF	Access Control Field
ACK	Acknowledgement
ACM	Address Complete Message
ACR	Allowed (or Available) Cell Rate
ACSE	Association Control Service Element
ACT	Activity Bit
ACTS	Advanced Communication Technologies and Services (in Europe)
ACTS	Advanced Communications Technology Satellite (in U.S.)
ADM	Add/Drop Multiplexer
ADMD	ADministrative Management Domain
ADPCM	Adaptive Differential Pulse Code Modulation
ADSL	Asymmetric Digital Subscriber Line
ADTF	ACR Decrease Time Factor
AE	Application Element
AEI	Application Entity Identifier
AFI	Address Format Identifier / Authority and Format Identifier
AHFG	ATM-attached Host Functional Group
AII	Active Input Interface
AIM	ATM Inverse Multiplexer
AIMS	Action team for the Integration of Management Systems

AIP	ATM Interface Processor
AIR	Additive Increase Rate
AIS	Alarm Indication Signal
AISE	Alarm Indication Signal - External
AIX	Advanced Interactive eXecutive
AMI	Alternate Mark Inversion
AMS	Audio/Visual Multimedia Services
ANI	Automatic Number Identification
ANM	ANswer Message
ANSI	American National Standards Institute
AOI	Active Output Interface
API	Application Programming Interface
APPC	Advanced Peer-to-Peer Communication
APPN	Advanced Peer-to-Peer Networking
ARA	Appletalk Remote Access
ARMA	Autoregressive Moving Average Process
ARP	Address Resolution Protocol
ARQ	Automatic Repeat reQuest
ARS	Amateur Radio Service
AS	Autonomous System
ASE	Application Service Element
ASIC	Application Specific Integrated Circuit
ASN	Abstract Syntax Notation
ASN.1	Abstract Syntax Notation One
ASP	Abstract Service Primitive
ATBCL	Average Time beween Cell Losses
ATD	Asynchronous Time Division
ATDM	Asynchronous Time Division Multiplexing
ATDnet	Advanced Technology Demonstration Network
ATE	ATM Terminating Equipment
ATF	Access Termination Function
ATM	Asynchronous Transfer Mode
ATMARP	ATM Address Resolution Protocol
ATMF	ATM Forum

ATMF SEC	ATM Forum Security Specification
ATM-PDU	ATM Physical Data Unit
ATM-SAP	ATM-Service Access Point
ATOM	ATM Output Buffer Modular
AToM MIB	IETF Working Group for MIBs based on SNMP and ATM
ATS	Abstract Test Suite
AU	Administrative Unit
AUG	Administrative Unit Group
AUI	Attachment Unit Interface
AUU	ATM User-to-User
AVD	Adaptive Voice/Data Network
AVSSCS	Audio-Visual Service Specific Convergence Sublayer
AWACS	ATM Wireless Access Communication System

BAHAMA	Broadband Adaptive Homing ATM Architecture
BASize	Buffer Allocation Size
BBC	Broadband Bearer Capability
BC	Bearer Control
BCC	Bearer Connection Control
BCD	Binary Coded Decimal
BCDBS	Broadband Connectionless Data Bearer Service
BCDS	Broadband Connectionless Data Service
BCN	Broadcast Channel Number
BCOB	Broadband Class of Bearer
BEC	Backward Error Correction
BECN	Backward Explicit / Error Congestion Notification
BELLCORE	Bell Communications Research
BER	Bit Error Rate / Basic Encoding Rules
BGP	Border Gateway Protocol
BGT	Broadcast and Group Translators
BHCA	Busy Hour Call Attempt
BHLI	Broadband High Layer Information
BIB	Backward Indicator Bit

B-ICI	Broadband Inter-Carrier Interface
BIOS	Basic Input/Output System
BIP	Bit Interleaved Parity / Broadband Intelligent Peripheral
BIPV	Bit Interleaved Parity Violation
BIS	Border Intermediate System
B-ISDN	Broadband Integrated Services Digital Network
B-ISSI	Broadband Inter-Switching System Interface
B-ISUP	Broadband Integrated Services User Part / B-ISDN User Part
BLLI	Broadband Low Layer Information
BNT	Broadband Network Termination
BNT1	Broadband Network Termination 1
BNT2	Broadband Network Termination 2
BoM	Beginning of Message
BOOTP	Bootstrap Protocol
BPDU	Bridge Protocol Data Unit
BPP	Bridge Port Pair
BPS	Bits per second
BRI	Basic Rate Interface
BSCP	Broadband Service Control Point
BSD	Berkeley Standard Distribution
BSN	Backward Sequence Number
BSS	Broadband Switching System
BSSP	Broadband Service Switching Point
BSVC	Broadcast Switched Virtual Connections
BT	Burst Tolerance
BTA	Broadband Terminal Adaptor
BTAG	Begin Tag
BTE	Broadband Terminal Equipment
BUS	Broadcast and Unknown Server
BW	Bandwidth

CA	Cell Arrival
CAC	Connection/Call Admission Control

CAD	Computer Aided Design
CAM	Computer Aided design Manufacturing
CAS	Channel Associated Signaling
CASE	Computer Aided Software Engeneering
CAT3	Category 3 Unshielded Twisted Pair
CAT5	Category 5 Unshielded Twisted Pair
CATV	Cable Television
CBC	Cipher Block Chaining
CBC-MAC	CBC Message Authentication Code
CBDS	Connectionless Broadband Data Service
CBER	Cell Block Error Ratio
CBR	Constant (or Continuous) Bit Rate
CC	Continuity Cell / Call Control
C^4I	Command, Control, Communications, Computer and Intelligence
CCF	Cross Correlation Function
CCITT	International Telegraph and Telephone Consultative Committee (Comité Consultatif International Télégraphique et Téléphonique)
CCR	Current Cell Rate
CCS	Common Channel Signaling
CCSS7	Common Channel Signaling System 7
CDF	Cutoff Decrease Factor
CDPD	Cellular Digital Packet Data
CDR	Cell Rate Decoupling
CD-ROM	Compact Disk Read Only Memory
CDS	Cell Directory Services
CDV	Cell Delay Variation
CDVT	Cell Delay Variation Tolerance
CEC	Common Equipment Card
CEI	Connection Endpoint Identifier
Cell	Basic ATM transmission unit
CEQ	Customer EQuipment
CER	Cell Error Ratio
CERN	Centre Europeen pour la Recherche Nucleaire
CERT	Computer Emergency Response Team
CES	Circuit Emulation Service

CI	Congestion Indication / Connection Identifier
CID	Configuration, Installation & Distribution
CIDR	Classless Inter-Domain Routing
CIF	Cells in Frames
CIK	Crypto-Ignition Key
CIO	Chief Information Officer
CIP	Carrier Identification Parameter
CIPSO	Common IP Security Option
CIR	Cell Insertion Rate / Committed Information Rate
CIV	Cell Interarrival Variation
CL	Connectionless
CLIP	Calling Line Identification Presentation
CLIR	Calling Line Identification Restriction
CLLM	Consolidated Link Layer Management
CLNAP	ConnectionLess Network Access Protocol
CLNIP	ConnectionLess Network Interface Protocol
CLNP	ConnectionLess Network Protocol
CLNS	ConnectionLess Network Service
CLON	ConnectionLess Overlay Network
CLP	Cell Loss Priority
CLR	Cell Loss Ratio
CLS	ConnectionLess Server
CLSF	ConnectionLess Service Function
CLTS	ConnectionLess Transport Service
CME	Component Management Entity / Conformant Management Entity
CMI	Coded Mark Inversion
CMIP	Common Management Information Protocol
CMIS	Common Management Information Services
CMISE	Common Management Information Service Element
CMOL	CMIP Management Over logical Link control
CMOT	CMIP Management Over TCP/IP
CMR	Cell Misinsertion Ratio
CN	Customer Network
CNAME	Canonical Name

CNM	Customer Network Management
CNR	Complex Node Representation
CO	Central Office / Connection Oriented
COD	Connection Oriented Data
COLP	Connected Line Identification Presentation
COLR	Connected Line Identification Restriction
CoM	Continuation of Message
CON	CONcentrator
CORBA	Common Object Request Broker Architecture
CoS	Class of Service
COSE	Common Open Software Environment
COSINE	Cooperation for OSI Networking in Europe
COTS	Connection Oriented Transport Service / Commercial Off The Shelf
CP	Connection Processor
CPCS	Common Part Convergence Sublayer
CPCS-CI	CPCS Congestion Indication
CPCS-LP	CPCS Loss Priority
CPCS-UU	CPCS User-to-User Indicator
CPE	Customer Premise Equipment
CPG	Call Progress
CPI	Common Part Indicator
CPN	Calling Party Number / Customer Premises Network
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check / Cyclic Redundancy Code
CRCG	Common Routing Connection Group
CRF	Connection Related Function
CRL	Certificate Revocation List
CRM	Cell Rate Margin
CRS	Cell Relay Service
CRV	Call Reference Value
CS	Capability Set / Carrier Selection / Convergence Sublayer
CS1	Capability Set One
CS2	Capability Set Two
CSF	Cell Switch Fabric

CSI	Convergence Sublayer Indication
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
CSPDN	Circuit Switched Public Data Network
CSPDU	Convergence Sublayer Protocol Data Unit
CSR	Cell Missequenced Ratio
CSU	Channel Service Unit
CTD	Cell Transfer Delay
CTS	Common Transport Semantics / Clear To Send
CTV	Cell Tolerance Variation
CUG	Closed User Group

DA	Destination Address
DAB	Digital Audio Broadcast
DAC	Dual Attached Concentrator
DARPA	Defense Advanced Research Projects Agency
DAS	Dual Attached Station
DAVIC	Digital Audio-Visual Council
DAWN	Demonstrator of Advanced Wireless Network
DBR	Deterministic Bit Rate
DCC	Data Country Code
DCE	Data Circuit-terminating Equipment / Distributed Computing Environment /Date Communication Equipment
DCF	Distributed Coordination Function
DCN	Data Communication Network
DCR	Dynamically Controlled Routing
DD	Depacketization Delay
DDCMP	Digital Data Communication Message Protocol
DDI	Direct-Dialling-In
DECT	Digital European Cordless Telephone System
DES	Data Encryption Standard / Destination End System
DES40	DES with 40 bit effective key
DFA	DXI Frame Address
DFI	Domain Specific Part Format Identifier

DFS	Distributed File Service
DFWMAC	Distributed Foundation Wireless MAC Protocol
DHCP	Dynamic Host Control Protocol
DIB	Directory Information Base
DISA	Defense Information Systems Agency
DISC	DISConnect
DIT	Directory Information Tree
DLC	Data Link Control
DLCI	Data Link Connection Identifier
DLL	Dial Long Lines
DMA	Direct Memory Access
DMDD	Distributed Multiplexing Distributed Demultiplexing
DME	Distributed Management Environment
DMI	Desktop Management Interface / Definition of Management Information
DN	Distribution Network
DNA	Digital Network Architecture
DNHR	Dynamic Nonhierarchial Routing
DNS	Domain Name System/Service
DOMS	Distributed Object Management System
DoD	Department of Defense
DPC	Destination Point Code
DPCM	Differential Pulse Code Modulation
DQDB	Distributed Queue Dual Bus
DQRUMA	Distributed-Queuing Request Update Multiple Access
DRAM	Dynamic Random Access Memory
DREN	Defense Research and Engineering Network
DS	Distributed Single Layer Test Method
DS-0	Digital Signal Level 0
DS-1	Digital Signal Level 1 (1.544 Mbit/s)
DS-2	Digital Signal Level 2 (6.312 Mbit/s)
DS-3	Digital Signal Level 3 (44.736 Mbit/s)
DSA	Directory System Agent / Dynamic Slot Assignment / Digital Signature Algorithm
DSAP	Destination Service Access Point
DSE	Distributed Single Layer Embedded Test Method

DSID	Destination Signaling Identifier
DSL	Digital Subscriber Line
DSP	Domain Specific Part
DSS	Digital Subscriber Signaling System / Digital Signature Standard
DSS1	Setup Digital Subscriber Signaling #1
DSS2	Setup Digital Subscriber Signaling #2
DSU	Data Service Unit
DSX	Digital Signal Cross-Connect
DTD	Document Type Definition
DTE	Data Terminal Equipment
DTL	Designated Transit List
DTLIE	DTL Information Element
DTS	Distributed Time Service
DUA	Directory User Agent
DUP	Data User Part
DVB	Digital Video Broadcast
DVMRP	Distance Vector Multicast Routing Protocol
DXC	Digital Cross-Connect
DXI	Data eXchange Interface

E1	European Digital Signal 1 (2.048 Mbit/s)
E3	European Digital Signal 3 (34.368 Mbit/s)
EBCDIC	Extended Binary Coded Decimal Interchange Code
EBCI	Explicit Backward Congestion Indication
EBCN	Explicit Backward Congestion Notification
ECB	Electronic Code Book
ECC	Elliptic Curve Cryptosystem
ECSA	Exchange Carriers Standards Association
EDFG	Edge Device Functional Group
EFCI	Explicit Forward Congestion Indication
EFCN	Explicit Forward Congestion Notification
EGP	Exterior Gateway Protocol
EIA	Electronic Industries Association

EIGRP	Enhanced IGRP
EISA	Enhanced Industry Standard Architecture
ELAN	Emulated Local Area Network
EMC	Electro Magnetic Compatibility
EMI	Electro Magnetic Interference
EML	Element Management Level
EMS	Element Management Systen
EN	Edge Node
ENR	Enterprise Network Roundtable
EoB	End of Bus
EoM	End of Message
EPD	Early Packet Discard
EPRCA	Enhanced Proportional Rate Control Algorithm
ER	Explicit Rate
ERIP	Extended RIP
ERM	Explicit Rate Marking
ES	End System / Edge Switch
ESF	Extended Super Frame
ESI	End System Identifier
ESIG	European SMDS Interest Group
ESIGN	Efficient Digital Signature Scheme
ET	Exchange Terminator
ETAG	End Tag
ETE	End-to-End
ETSI	European Telecommunications Standards Institute
EXM	Exit Message

FBR	Fixed Bit Rate
FC	Feedback Control / Fiber Connector
FCC	U.S. Federal Communications Commission
FCS	Fast Circuit Switching / Frame Check Sequence
FCVC	Flow Controlled Virtual Circuit
FDDI	Fiber Distributed Data Interface

FDM	Frequency Division Multiplexing
FDMA	Frequency Division Multiple Access
FE	Front-End
FEA	Functional Entity Action
FEAL	Fast Data Encipherment Algorithm
FEBE	Far End Block Error
FEC	Forward Error Correction
FECN	Forward Explicit/Error Congestion Notification
FERF	Far End Receive Failure/Far End Reporting Failure
FG	Functional Group
FIB	Forward Indicator Bit
FIFA	First In, First Allocated
FIFO	First In, First Out
FR	Frame Relay
FRAD	Frame Relay Assembler Disassembler
FRF	Frame Relay Forum
FRM	Fast Resource Management
FRS	Frame Relay Service
FTAM	File Transfer Access & Management
FTP	File Transfer Protocol
FTTB	Fiber To The Building
FTTC	Fiber To The Curb
FTTH	Fiber To The Home
FUNI	Frame-based User-to-Network Interface

GAP	Generic Address Parameter
GCAC	General Call Admission Control
GCID	Global Call Identifier
GCIDIE	Global Call Identifier - Information Element
GCRA	Generic Cell Rate Algorithm
GDMO	Guidelines for the Definition of Managed Objects
GDS	Global Directory Services
GFC	Generic Flow Control

GHz	Giga Hertz
GIBN	Global Interoperability in Broadband Networks
GIPR	Gigabit IP Router
GMDP	Generally Modulated Deterministic Process
GOSIP	Government OSI Profile
GPS	Global Positioning System
GRC	Generic Reference Configuration
GSM	Global System for Mobile Communications
GUI	Graphical User Interface

HBFG	Host Behavior Functional Group
HCS	Header Check Sum/Sequence
HDB3	High Density Bipolar 3
HDLC	High Level Data Link Control
HDTV	High Definition TeleVision
HEC	Header Error Check / Header Error Control
HEL	Header Extension Length
HFC	Hybrid Fiber-Coax
HIPERLAN	High Performance Radio LAN
HIPNET	Multiservice Internet Protocols for High Performance Networks
HLF	Higher Layer Function
HLPI	Higher Layer Protocol Identifier
HLR	Home Location Register
HMI	Hub Management Interface
HODSP	High Order - Domain Specific Part
HoB	Header of Bus
HoL	Head-of-Line
HSSI	High-Speed Serial Interface
HSTP	High-Speed Transport Protocol
HTML	HyperText Markup Language
HTTP	HyperText Transfer Protocol

IA	Implementation Agreement
IAA	Initial Address Acknowledgment
IAB	Internet Activities Board
IAM	Initial Address Message
IANA	Internet Assigned Numbers Authority
IAR	Initial Address Reject
IASG	Internetwork Address Sub-Group
IBC	Integrated Broadband Communications
IBP	Interrupted Bernoulli Process
IBSG	Internetwork Broadcast Sub-Group
IBUFG	Internetwork Broadcast/Unknown Functional Group
IC	Initial Cell Rate
ICD	International Code Designator
ICFG	IASG Coordination Function Group
ICIP	Intercarrier Service Protocol
ICMP	Internet Control Message Protocol
ICR	Initial Cell Rate
IDI	Initial Domain Identifier
IDL	Interface Definition Language
IDP	Internet Datagram Protocol / Initial Domain Part
IDPR	InterDomain Policy Routing
IDRP	InterDomain Routing Protocol
IDU	Interface Data Unit
IE	Information Element
IEC	Inter-Exchange Carrier
IEEE	Institute of Electrical and Electronic Engineers
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IGRP	Interior Gateway Routing Protocol
IISP	Interim Inter-switch Signaling Protocol
ILMI	Integrated Layer Management Interface
IMA	Inverse Multiplexing for ATM
IME	Interface Management Entity
InfoWin	Information Window (ACTS)

IOP	Interoperability
IP	Internet Protocol / Intelligent Peripheral
IPP	Interrupted Poisson Process
IPNNI	Integrated Private Network to Network Interface
IPX	Internetwork Packet eXchange
IPng	IP next generation
IPv6	IP Version 6
IS	Intermediate System / International Standard
ISAG	Internet Address Summerazition Group
ISCP	ISDN Signaling Control Part
ISDN	Integrated Services Digital Network
ISL	Inter-Switch Link Protocol
ISLAN	Integrated Services LAN
ISO	International Standards Organization
ISP	International Standardized Profile / Internet Service Provider
ISUP	Integrated Services User Part / ISDN User Part
ISV	Independant Software Vendor
ITTC	Information and Telecommunication Technology Center, University of Kansas
ITU	International Telecommunication Union
ITU-T	ITU Telecommunication Standardization Sector
ITU-TSS	ITU Telecommunication Standardization Sector
IUT	Implementation Under Test
IWF	Interworking Function
IWU	InterWorking Unit
IXC	Inter-Exchange Carrier

JMCOMS	Joint Maritime Communication System
JDE	JMCOMS Joint Development Environment
JITC	Joint Interoperability Test Command
JPEG	Joint Photographic Experts Group

kbit/s	Kilo bit/s

KHz	Kilo Hertz

LAN	Local Area Network
LANE	LAN Emulation
LAPB	Link Access Procedure Balanced
LAPD	Link Access Procedure D
LAPF	Link Access Procedure F
LAT	Local Area Transport
LATA	Local Access and Transport Area
LB	Leaky Bucket
LCD	Loss of Cell Delineation
LCN	Logical Channel Number
LCP	Link Control Protocol
LCT	Last Cell Compliance Time
LD	LAN Destination
LE	LAN Emulation
LEARP	LAN Emulation Address Resolution Protocol
LEC	LAN Emulation Client / Local Exchange Carrier
LECID	LAN Emulation Client Identifier
LECS	LAN Emulation Configuration Server
LED	Light Emitting Diode
LENNI	LAN Emulation Network Node Interface
LES	LAN Emulation Server
LGN	Logical Group Node
LI	Length Indication
LIJP	Leaf Initiated Join Parameter
LIS	Logical IP Subnetwork
LIV	Link Integrity Verification
LLATMI	Lower Layer ATM Interface
LLC	Logical Link Control
LLID	Loopback Location Identification
LME	Layer Management Entity
LMI	Local Management Interface

LNNI	LAN Emulation Network-Node Interface / LAN Emulation Network-to-Network Interface
LoC	Loss of Cell delineation
LoF	Loss of Frame
LoP	Loss of Pointer
LoS	Loss of Signal / Line of Sight
LSAP	Link Service Access Point
LSB	Least Significant Bit
LSP	Link State Protocol
LSR	Leaf Setup Request
LSS	Link Status Signal
LSU	Link State Update
LT	Line Terminator / Lower Tester
LTE	Line Terminating Equipment
LTH	Length Field
LUNI	LAN Emulation UNI (User Network Interface)

MA	Maintenance and Adaptation
MAC	Medium Access Control
MAGIC	Multidimensional Applications and Gigabit Internetwork Consortium
MAN	Metropolitan Area Network
MAP	Mobile Application Part
MAPDU	Management Application Protocol Data Unit
MARS	Multicast Address Resolution Server
MAU	Medium Attachment Unit / Multistation Access Unit
Mbit/s	Mega bit/s
MBONE	Multicasting backBONE
MBS	Maximum Burst Size / Mobile Broadband System
MCDV	Maximum Cell Delay Variation
MCLR	Maximum Cell Loss Ratio
MCNC	Microelectronics Center of North Carolina
MCR	Minimum Cell Rate
MCTD	Maximum Cell Transfer Delay / Mean Cell Transfer Delay
MD5	Message Digest algorithm 5

MDPDU	Management Data PDU
ME	Mapping Entity
MEDIAN	Wireless Professional and Residential Multimedia Applications
MHz	Mega Hertz
MIB	Management Information Base
MICE	Multimedia Integrated Conferencing for European Researchers
MID	Multiplexing Identifier / Message Identifier
MIL-STD	Military Standard
MIME	Multipurpose Internet Mail Extensions
MIN	Multistage Interconnection Network
MIPS	Mega Instructions Per Second
MIR	Maximum Information Rate
MISSI	Multi-level Information System Security Initiative
MMF	Multimode Fiberoptic cable
MMIC	Monolithic Microwave Integrated Circuits
MMPP	Markov Modulated Poisson Process
MOCS	Managed Object Conformance Statement
MoM	Manager of Managers
MONET	High Data Rate Mobile Internet
MOP	Meta Object Protocol
MOSPF	Multicast OSFP
MPDU	MAC Protocol Data Unit
MPEG	Moving Picture Experts Group
MPH	Miles Per Hour
MPL	Maximum Packet Length / Maximum Packet Lifetime
MPOA	MultiProtocol Over ATM
MPX	MultiPleXer
MR	Mean Rate
MRCS	Multi-Rate Circuit Switching
MS	Meta Signaling
MSAP	Management Service Access Point
MSB	Most Significant Bit
MSN	Multiple Subscriber Number
MSN-CMA	Multi-Service Network Connection Management Architecture

MSOH	Multiplex Section OverHead
MSDU	MAC Service Data Unit
MSU	Message Signal Unit
MSVC	Meta-signaling Virtual Channel
MT	Message Type
MTA	Message Transfer Agent
MTP	Message Transfer Part
MTU	Maximum Transmission Unit
MUX	Multiplexer
MX	Moving Window
MXRR	Mail eXchange Resource Record

NACK	Negative ACKnowledgement
NBMA	Non-Broadcast Multiple Access
NCP	Network Control Protocol
NCSA	National Center for Supercomputing Applications
NDIS	Network Driver Interface Specification
NDS	Netware Directory Service
NE	Network Element
NEBIOS	Network Basic Input Output System
NETBLT	Network Block-Transfer Protocol
NEXT	Near End Crosstalk
NFS	Network File System
NH	National Host
NHF	National Host Forum
NHRP	Next Hop Resolution Protocol
NHS	Next Hop Server
NI	Network Indicator
NIC	National/Network Information Centre / Network Interface Card/Controller
NIP	Network Integrated Processing
NIS	Network Information System
NISDN	Narrowband Integrated Services Digital Network
NIST	National Institute of Standards and Technology (in U.S.)

NIU	Network Interface Unit
NLM	Netware Loadable Module
NLPID	Network Layer Protocol Identifier
NLSP	NetWare Link State Protocol
NME	Network Management Entity
NMF	Network Management Forum
NML	Native Mode LAN / Network Management Level
NMS	Network Management System
NNI	Network Node Interface or Network-to-Network Interface
NNTP	Network News Transfer Protocol
NOC	Network Operation Center
NOS	Network Operating System
NP	Network Performance
NPC	Network Policing Control / Network Parameter Control
NPM	Network Processor Module
NRM	Network Resource Management
NRN	National Research Network
NRT-VBR	Non-Real-Time VBR
NSA	National Security Agency
NSAP	Network Service Access Point
NSC	National Support Center
NSF	National Science Foundation
NSP	Network Service Provider
NSR	Non-Source Routed
NT	Network Termination
NT1	Network Termination 1
NT2	Network Termination 2
NTF	Network Termination Function
NTP	Network Termination Point / Network Time Protocol
NTSC	National Television System Committee
NVP	Nominal Velocity of Propagation
NVOD	Near Video On Demand

OAM	Operation, Administration, and Maintenance
OAMP	Operation, Administration, Maintenance, and Provisioning
OC-n	Optical Carrier (n=3,12,48,....)
OCD	Out-of-Cell Delineation
ODA	Office (or Open) Document Architecture
ODI	Open Data link Interface
ODIF	Office Document Interchange Format
ODLI	Open Data Link Interface
OEM	Original Equipment Manufacturer
OFDM	Orthogonal Frequency Division Multiplex
OIM	OSI Internet Management
OLI	Originating Line Information
OME	Object Management Edge
OMG	Object Management Group
OMAP	Operations Maintenance and Administration Part
OMSN	Open Multi Service Network
ONC	Open Network Computing
ONP	Open Network Provisions
OOA	Object Oriented Analysis
OOD	Object Oriented Design
OoF	Out of Frame
OOP	Object Oriented Programming
OPC	Origin Point Code
OPCR	Original Program Clock Reference
ORB	Object Request Broker
ORL	Olivetti Research Limited
OS	Operation System
OSF	Open Software Foundation
OSI	Open Systems Interconnection
OSID	Origination Signaling Identifier
OSIRM	Open Systems Interconnection Reference Model
OSPF	Open Shortest Path First
OSS	Operation Support System
OSSA	Open Service Support Architecture

OUI	Organizationally Unique Identifier

PABX	Private Automatic Branch eXchange
PAD	Packet Assembler and Disassembler
PAM	Pulse Amplitude Modulation
PAR	Positive Acknowledgement with Retransmission
PARIS	Packetized Automated Routing Integrated System
PBX	Private Branch eXchange
PBS	Portable Base Station
PC	Priority Control / Personal Computer
PCB	Protocol Control Block
PCF	Point Coordination Function
PCI	Protocol Control Information
PCM	Pulse Code Modulation
PCO	Point of Control and Observation
PCR	Peak Cell Rate
PCRA	Proportional Rate-Control Algorithm
PCS	Public Communication System / Personal Communications Services
PCVS	Point to Point Switched Virtual Connections
PD	Packetization Delay
PDH	Plesiochronous Digital Hierarchy
PDU	Protocol Data Unit
PEAN	Pan-European ATM Network
PEM	Privacy Enhanced Mail
PES	Packetized Elementary System
PGL	Peer Group Leader
PGP	Pretty Good Privacy
PHS	Personal Handy-phone System
PHY	Physical Layer
PHYSAP	Physical Layer Service Access Point
PI	Protocol Identifier
PICS	Protocol Implementation Conformance Statement
PID	Protocol Identifier Governing Connection Types

PIM	Protocol Independant Multicast
PIR	Packet Insertion Rate
PIXIT	Protocol Implementation eXtra Information for Testing
PL	Physical Layer
PLCP	Physical Layer Convergence Procedure/Protocol
PLIM	Physical Layer Interface Module
PLL	Phase Locked Loop
PLOU	Physical Layer Overhead Unit
PLR	Packet Loss Rate
PLSP	PNNI Link State Packets
PM	Physical Medium / Performance Monitoring
PMD	Physical Medium Dependent
PMP	Point to Multipoint
PNNI	Private Network Node Interface or Private Network-to-Network Interface
PNO	Public Network Operator
POH	Path OverHead
POI	Path Overhead Indicator
PON	Passive Optical Network
PoP	Point of Presence
POSIX	Portable Operating System for UNIX
PPD	Partial Packet Discard
PPP	Point-to-Point Protocol
PRI	Primary Rate Interface
PRM	Protocol Reference Model
PRMA	Packet Reservation Multiple Access
PRMD	PRivate Management Domain
PROM	Programmable ReadOnly Memory
PS	Program stream
PSTN	Public Switched Telephone Network
PT	Payload Type
PTE	Path Terminating Equipment
PTI	Payload Type Identifier
PTM	Packet Transfer Mode
PTO	Public Telecommunications Operator

PTSE	PNNI Topology State Element
PTSP	PNNI Topology State Packet
PTT	Post, Telegraph, and Telephone
PUNI	Private User Network Interface
PVC	Permanent Virtual Channel / Permanent Virtual Connection
PVCC	Permanent Virtual Channel Connection
PVP	Permanent Virtual Path
PVPC	Permanent Virtual Path Connection
PWI	Public Windows Interface
PWS	Personal WorkStation

Q3,Qx,X,F,G	Standardized Interfaces in TMN networks
QA	Q-Adapter
QAM	Quadrature Amplitude Modulation
QCIF	Quarter-CIF
QD	Queuing Delay
QFC	Quantum Flow Control
QoS	Quality of Service
QPSK	Quadrature Phase Shift(ed) Keying
QPSX	Queue Packet and Synchronous Circuit Exchange

RACE	Research on Advanced Communications in Europe
RAI	Remote Alarm Indication
RAL	Radio Access Layer
RARE	Reseaux Associes pour la Recherche Europeenne
RBOC	Regional Bell Operating Company
RC	Request Counter / Routing Control
RD	Route Descriptor / Routing Domain
RDF	Rate Decrease Factor
RDI	Remote Defect Indication
RDRN	Rapidly Deployable Radio Network
REL	Release

RES	Reserved Field
RF	Radio Frequency
RFC	Request For Comment
RFI	Radio Frequency Interference
RI	Routing Information
RIF	Rate Increase Factor / Routing Information Field
RII	Routing Information Indicator
RIP	Routing Information Protocol
RIPE	Reseaux IP Europeenne
RISC	Reduced Instruction Set Computer
RLC	Release Complete
RM	Resource Management
RMON	Remote MONitoring
RN	Remote Node
ROLC	Routing Over Large Clouds
ROSE	Remote Operations Service Element
RPC	Remote Procedure Call
RR	Relative Rate in ABR
RS	Regenerator Section
RSA	Rivest, Shamir, and Adleman (algorithm)
RSFG	Route Server Functional Group
RSOH	Regenerator Section OverHead
RSVP	ReSerVation Protocol / Resource Reservation Protocol
RT	Routing Type
RTCP	Real Time Control Protocol
RTMP	Routing Table Maintenance Protocol
RTP	Real Time Protocol
RTS	Residual Time Stamp / Request To Send / Ready To Send
RTSP	Real Time Streaming Protocol
RTT	Round-Trip Time
RTTI	RunTime Type Identification
RT-VBR	Real-Time VBR

SA	Source Address
SAA	System Application Architecture
SAAL	Signaling ATM Adaptation Layer
SABM	Set Asynchronous Balanced Mode
SAC	Single Attached Concentrator
SACF	Single Association Control Function
SAMBA	System for Advanced Mobile Broadband Applications
SAME	System Management Application Entity
SAO	Single Association Object
SAP	Service Access Point / Service Advertising Protocol
SAPI	Service Access Point Identifier
SAR	Segmentation and Reassembly
SARPDU	Segmentation and Reassembly Protocol Data Unit
SAS	Single Attached Station
SBR	Statistical Bit Rate
SBBP	Switched Batch Bernoulli Process
SC	Subscriber Connector / Switching Center
SCCP	Signaling Connection Control Part
SCI	Secure Compartmented Information
SCP	Service Control Point / Switch Control Processor
SCPS	Synchronous Composite Packet Switching
SCR	Sustainable/Sustained Cell Rate
SDH	Synchronous Digital Hierarchy
SDI	Storage Device Interface
SDL	Specification Description Language
SDLC	Synchronous Data Link Control
SDPDU	Sequenced Data PDU
SDPPDU	Sequenced Data with Poll PDU
SDT	Structured Data Transfer
SDU	Service Data Unit
SE	Switching Element
SEAL	Simple and Efficient Adaptation Layer
SECB	Severely Errored Cell Block
SEL	SELector

SES	Source End Station
SF	Switching Fabric
SFET	Synchronous Frequency Encoding Technique
SFI	System Format ID
SFMA	Specific Functional Management Areas
SGM	Segmentation Message
SGML	Standard Generalized Markup Language
SHA	Secure Hash Algorithm
SHD	Super High Definition (television)
SI	Service Indicator
SID	Signaling Identifier
SIF	Signaling Information Field
SIG	Special Interest Group
SIO	Service Information Field
SIP	SMDS Interface Protocol
SIPP	Simple Internet Protocol Plus
SIR	Sustained Information Rate
SKC	Session Key Changeover
SKE	Session Key Exchange
SLC	Signaling Link Code
SLIP	Serial Line Internet Protocol
SLS	Signaling Link Selection
SMAE	System Management Application Entities
SMC	Sleep Mode Connection
SMDR	Storage Management Data Requester
SMDS	Switched Multi-Megabit Data Service
SME	Storage Management Engine / Security Message Exchange
SMF	Single Mode Fiber / System Management Function
SMFA	Specific Management Functional Areas
SMI	Structure of Management Information
SMS	Storage Management Service / Switched Management System
SMT	Synchronous Multiplex Terminal
SMTP	Simple Mail Transfer Protocol
SN	Sequence Number

SNA	Systems Network Architecture
SNAP	SubNetwork Access Point/Protocol / Subnetwork Attachment Point
SNDCF	Sub-Network Dependent Convergence Function
SNI	Subscriber Network Interface
SNMP	Simple Network Management Protocol
SNP	Sequence Number Protection
SOH	Section OverHead
SONET	Synchronous Optical NETwork
SP	Signaling Point
SPANS	Simple Protocol for ATM Network Signaling
SPE	Synchronous Payload Envelope
SPF	Shortest Path First
SPID	Service Protocol Identifier
SPTS	Single Program Transport Stream
SPVC	Soft Permanent Virtual Circuit / Switched or Semi-Permanent Virtual Connection
SPX	Sequenced Packet eXchange
SR	Source Routing
SREJ	Selective Reject
SRF	Specifically Routed Frame
SRT	Source Routing Transparent
SRTS	Synchronous Residual Time Stamp
SS7	Signaling System Number 7
SSAP	Source Service Access Point
SSCF	Service Specific Coordination Function
SSCOP	Service Specific Connection-Oriented Protocol
SSCP	Systems Services Control Point
SSCS	Service Specific Convergence Sublayer
SSM	Single-Segment Message
SSP	Service Switching Point
SSRC	Synchronization Source Identifier
SSS	Self Synchronizing Scrambler
ST	Segment Type
STB	Set-top Box
STC	Sinusoidal Transform Coder

STD	Synchronous Time Division
STDM	Statistical/Synchronous Time-Division Multiplexing
STE	Section Terminating Equipment / Spanning Tree Explorer
ST-II	STream protocol version II
STM	Synchronous Transfer Mode
STM-1	Synchronous Transport Module-1
STM-n	Synchronous Transport Module-n
STP	Shielded Twisted Pair / Signaling Transfer Point
STS	Synchronous Time Stamps / Synchronous Transport Signal
STS-1	Synchronous Transport Signal-1
STS-3c	Synchronous Transport System-Level 3 concatenated
STS-n	Synchronous Transport Signal-n
SUT	System Under Test
SVB	Switched Video Broadcasting
SVC	Signaling/Switched Virtual Channel
SVCI	Switched Virtual Channel Identifier
SVP	Switched Virtual Path
SWAN	Seamless Wireless ATM Network
SWG	Sub-Working Group

T1	Transmission link level 1 (1.536 Mbit/s)
T1S1	ANSI T1 Subcommittee
T3	Transmission link level3
TA	Terminal Adapter
TAT	Theoretical Arrival Time
TAXI	Transparent Asynchronous Transmitter/Receiver Interface
TB	Transparent Bridging
TC	Transaction Capabilities / Transmission Convergence
TCAP	Transaction Capabilities Application Part
TCB	TCP Control Block / Trusted Computer Base
TCI	Test Cell Input
TCO	Test Cell Output
TCP	Transmission Control Protocol

TCP/IP	Transmission Control Protocol/Internet Protocol
TCRF	Transit Connection Related Function
TCS	Transmission Convergence Sublayer
TDD	Timing Data Distribution
TDJ	Transfer Delay Jitter
TDM	Time-Division Multiplexing
TDMA	Time Division Multiple Access
TE	Terminal Equipment
TEI	Terminal Equipment Identifier
TEN	Trans-European Networks
TERENA	Trans-European Research and Education Networking Association
TFTP	Trivial File Transfer Protocol
TIES	Telecom Information Exchange Services
TIG	Topology Information Group
TJW	Triggered Jumping Window
TM	Traffic Management
TM SWG	Traffic Management Sub-Working Group
TMN	Telecommunication Management Network
TMP	Test Management Protocol
TNS	Transit Network Selection
TP	Terminal Portability / Twisted Pair
TP4	Transport Protocol Class 4
TPCC	Third Party Call Control
TPD	Trailing Packet Discard
TPDU	Transport Protocol Data Unit
TPE	Transmission Path Endpoint
TRD	Transit Routing Domain
TS	Time Slot / Time Stamp / Traffic Shaping / Transport Stream / Top Secret
TSA	Target Service Agent
TSAP	Transport Service Access Point
TSDU	Transport Service Data Unit
TTS	Trouble Ticket System
TU	Tributary Unit
TUC	Total User Cell count

TUCD	Total User Cell Difference
TUG	Tributary Unit Group
TUGn	Tributary Unit Group
TULIP	TCP and UDP over Lightweight IP
TUNIP	TCP and UDP over non-existent IP
TUP	Telephone User Part
TUn	Tributary Unit
TVOD	True Video On Demand

UA	Unnumbered Acknowledgement / User Agent
UBR	Unspecified Bit Rate
UBR+	Unspecified Bit Rate Plus
UDP	User Datagram Protocol
UME	UNI Management Entity
UMTS	Universal Mobile Telecommunication System
UNI	User-Network Interface
UNIX	Uniplexed Information and Computing System
UNMA	Unified Network Management Architecture
UPC	Usage Parameter Control / User Policing Control
UPR	Universal Receiver Protocol
URC	Uniform Resource Citation
URI	Universal Resource Identifier
URL	Uniform Resource Locator
URN	Uniform Resource Name
UT	Upper Tester
UTOPIA	Universal Test & Operation Physical Interface
UTP	Unshielded Twisted Pair
UUS	User-to-User Signaling

VAP	Value Added Process
VAR	Value Added Reseller
VBR	Variable Bit Rate

VBR-NRT	Variable Bit Rate - Non-Real Time
VBR-RT	Variable Bit Rate - Real Time
VC	Virtual Channel
VCC	Virtual Channel Connection
VCCI	Virtual Channel Connection Identifier
VCFC	Virtual Circuit Flow Control
VCI	Virtual Channel Identifier
VCL	Virtual Channel Link
VCn	Virtual Container n
VD	Virtual Destination
VF	Variance Factor
VFN	Vendor Feature Node
VLAN	Virtual Local Area Network
VLR	Visitor Location Register
VLSI	Very low scale integration
VMTP	Versatile Message Transaction Protocol
VOD	Video on Demand
VP	Virtual Path
VP-AIS	VP-Alarm Indication Signal
VPC	Virtual Path Connection
VPCI	Virtual Path Connection Identifier
VP-FERF	VP Far-End Receive Failure
VPI	Virtual Path Identifier
VPL	Virtual Path Link
VPN	Virtual Private Network
VPT	Virtual Path Terminator
VS	Virtual Scheduling / Virtual Source
VT	Virtual Tributary
VTP	VLAN Trunk Protocol

WAIS	Wide Area Information Server
WAN	Wide Area Network
WAND	Wireless ATM Network Demonstrator

WATM	Wireless ATM
WFQ	Weighted Fair Queuing
WG	Working Group
WINS	Windows Internet Name Service
WLL	Wireless Local Loop
WLAN	Wireless LAN
WORM	Write Once Read Many
WP	Work Package
WS	Workstation
WWW	World Wide Web

XDR	eXternal Data Representation
XMP	X/open Management Protocol
XNS	Xerox Network Systems
XOM	X/open OSI-abstract data Manipulation
XPG	X/open Portability Guide
XTP	eXpress Transport Protocol

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	September 1997	Final

4. TITLE AND SUBTITLE
ASYNCHRONOUS TRANSFER MODE (ATM)

5. FUNDING NUMBERS
PE: 0602232N
AN: DN305555
WU: R3211

6. AUTHOR(S)
R. L. Ehlen

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Command, Control and Ocean Surveillance Center (NCCOSC)
RDT&E Division (NRaD)
San Diego, California 92152–5001

8. PERFORMING ORGANIZATION REPORT NUMBER
TR 1754

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Office of Naval Research
800 North Quincy Street
Arlington, VA 22217–5660

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 words)*

This report describes the fast-evolving ATM technology, with special emphasis on new standards, research results, and developments.

14. SUBJECT TERMS
Mission Area: Command, Control, and Communications
Asynchronous Transfer Mode (ATM)
packet-switched networks

15. NUMBER OF PAGES
182

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	SAME AS REPORT